*Special Issue: Digital Face and Deep Fakes*

CONVERGENCE

# Rebalancing our regulatory response to Deepfakes with performers' rights

Convergence: The International Journal of Research into New Media Technologies
2021, Vol. 0(0) 974–998

DOI: 10.1177/13548565211033418
journals.sagepub.com/home/con


**Mathilde Pavis**
University of Exeter, UK

## Abstract

Law experts have been actively looking for solutions within the law to control Deepfakes since their emergence in 2017. This article puts forward performers' rights as a suitable regulatory tool for Deepfakes, defined as synthetic performances produced using artificial intelligence systems. In many respects, performers' rights represent a more sophisticated response to the challenges posed by Deepfake technology compared to existing legal remedies and reform proposals introduced to regulate Deepfakes. In making its case for performers' rights as suitable regulatory response to Deepfakes, this article uncovers a tension: performers' rights are an attractive solution to regulate Deepfakes but this technology challenges their scope of application. This is because Deepfakes uses content protected by performers' rights (performances) in a way unforeseen by intellectual property policy-makers at the time these rights were introduced into law. Despite this limitation, performers' rights remain one of the most attractive legal remedies in regulating Deepfakes, if adequately reformed. This article proposes two routes for the reform of performers' rights to address this gap. The first involves an ad hoc modification of performers' rights to ensure that performances manipulated by Deepfakes are covered. The second and preferred recommendation replaces the regime of performers' rights with a regime of performers' copyright. This small, yet important, change in legal regimes can be the difference between piecemeal, uneven and, therefore, ineffective protection against unauthorized Deepfakes and a harmonized international approach to the technology.

## Keywords

Deepfakes, performers' rights, intellectual property, law, performer, performance synthetisation, digital avatars, United Kingdom

## Introduction

Legal experts and policy-makers have been actively seeking solutions within the law to control Deepfakes since their emergence in 2017. In the context of this debate, this article develops a

**Corresponding author:**
Mathilde Pavis, University of Exeter, Amory Building, Rennes Drive, Streatham Campus, Exeter EX4 4RJ, UK.
Email: m.pavis@exeter.ac.uk

principled approach for a balanced regulatory response to Deepfakes, defined as synthetic performances produced using artificial intelligence (AI) systems.[1] This approach is put into practical application by proposing performers' rights as a suitable tool for the regulation of Deepfakes.

In many respects, performers' rights represent a more sophisticated response to the challenges posed by Deepfake technology compared to existing legal remedies or recent legislative proposals introduced to regulate Deepfakes. This is so for two key reasons. First, performers' rights are rights of international standing better equipped to respond to the global phenomenon of Deepfakes. Second, performers' rights provide a framework capable of handling legitimate Deepfakes, and Deepfakes authorized by the person depicted in them, instead of solely focusing on illegitimate or malicious applications of the technology, the approach of regulatory responses to date. In this regard, a solution in performers' rights contributes to re-balancing the framing of Deepfakes in the legal scholarship and policy-making.

Whilst performers' rights are an attractive solution to regulate Deepfakes, this technology also challenges their scope of application. This is because Deepfakes use content protected by performers' rights (performances) in a way unforeseen by intellectual property policy-makers at the time these rights were introduced into law.

A careful analysis of the AI systems used to create Deepfakes reveals that Deepfake technology achieves something no recording technology has done before: they are able to produce high-quality, low-budget, realistic *imitations* of performances on scale. The imitation, or reproduction, of a performance is not protected by performers' rights, or any other intellectual property right strictly speaking.

This article proposes the reform of performers' rights to address this gap to cover the reproduction, or imitation, of performances. This seemingly small, yet important, change in legal regimes can be the difference between piecemeal, uneven and, therefore, ineffective protection against unauthorized Deepfakes and a harmonized international response to the technology.

This article opens with a definition of Deepfakes and the underpinning technology to contextualize the analysis in law (*Definition and description of Deepfakes*). It then proposes a principled approach to the regulation of Deepfakes, which is then translated into a concrete benchmark for legal standards of protection (*A principled approach for a balanced regulatory response to Deepfakes*). Existing standards of protection for the Deepfaked person section uses this benchmark to review existing laws before demonstrating the contribution of performers' rights to improving standards of regulation applicable to Deepfakes (*Raising standards of protection for the Deepfaked person: a solution in performers' rights*). As little-known rights of intellectual property, this section describes performers' rights, highlighting their pertinence in controlling Deepfakes. The analysis exposes performers' rights' own limitation in controlling the imitation of performances, as with those generated by Deepfakes. This gap is addressed in the last section of the analysis which proposes two options for reforms under national and international law (*A reform of performers' rights*).

For the purpose of this discussion, the analysis engages with the laws applicable to England and Wales, and where appropriate the United Kingdom (UK), as its primary point of reference. This is so for three reasons. First, there are significant differences in the legal provisions applicable to Deepfakes between national laws, which cannot be accounted for jurisdiction by jurisdiction within the confines of this article. Second, the UK is a jurisdiction ripe for reform on the issue of Deepfakes as the government is undertaking a series of reviews in connected areas of law (UK Intellectual Property office, 2021, UK Law Commission, 2018; UK Intellectual Property Office, 2020). Third, surprisingly little has been written on Deepfakes in relation to UK law (Farish, 2020a, 2020b; O'Connell, 2020; O'Connell and Bakina, 2020; Perrot and Mostert, 2020; Pavis, 2020, 2021a) in

contrast to the volume of scholarship published on laws applicable in the United States (US) (e.g. Caldera, 2019; Chesney and D Citron, 2019a; Chesney and DK Citron, 2019b; Delfino, 2020; Franks and Waldman, 2019; Ice, 2019; Kirchengast, 2020; Kugler and Pace, 2021; Pechenik Gieseke, 2020; Silbey and Hartzog, 2019; Yamaoka-Enkerlin, 2020).

## Definition and description of Deepfakes

### *Definition*

'Deepfakes' (or 'Deep Fakes') are a type of synthetic performance created using AI systems known as neural networks (Pavis, 2020: 8; Mirsky and Lee, 2020). Deepfakes are synthetic performances that resemble an existing performance by re-using the likeness of the performer or the performance, or both. They most commonly take the form of videos or sound recordings that imitate the likeness of a person's face, voice or performance. Deepfakes manipulate real (authentic) footage of a person to generate a digital imitation.

Current 'AI systems' used to generate Deepfakes rely on machine-learning algorithms known as neural networks. The four key types of neural networks used include Encoder-Decoder Networks, Convolutional Neural Networks, Generative Adversarial Networks and Recurrent Neural Networks (Pavis, 2020: 8; Mirsky and Lee, 2020).

### *Application*

Typical purposes for generating Deepfakes include: the editing or enhancement of a performance; the re-enactment of a performance; the replacement of a performance by another and the creation of a completely new performance, also known as 'pure synthesis' (Mirsky and Lee, 2020; Pavis, 2020: 5–6).

Any of these purposes could be used for legitimate or illegitimate ends. Malicious applications of the technology have been usefully mapped out by Chesney and Citron (2019a) in their seminal piece on Deepfakes and laws applicable in the US. In this piece, the authors note the threat posed by Deepfakes to: individuals' autonomy and freedom from harm (via sexual abuse, harassment, blackmail, discrimination or defamation); democracy (via the manipulation of elections, disruptions of democratic processes through information disorder) and commercial integrity of individuals and organisations (via free-riding, passing off or commercial sabotage).

By contrast, legitimate applications of the technology may involve using Deepfakes to: entertain or produce artistic provocations, parodies, criticism or satire in the context of free speech (Chan et al., 2018; Lees, 2021); create more engaging educational resources (Chesney and Citron, 2019a); generate accessible content for differently-abled users (Westerlund, 2019); make content available in multi-languages (Meskys et al., 2020) or, offer new commercial services (Kwok and Koh, 2020; Kietzmann et al., 2020; Lees, 2021; Meskys et al., 2020).

### *Description*

This section does not aim to give a detailed account of how Deepfakes are generated using AI systems. Instead, it describes in simple terms key aspects of the synthetisation process of relevance to our legal analysis. A more detailed technical primer was given elsewhere (Pavis, 2020) and this section draws on that content. Other important work by AI experts will be useful to readers

interested in AI modelling for performance synthetisation (e.g. Misky and Lee, 2020; Chan et al., 2018; Deng et al., 2020; Zakharov et al., 2019).

AI systems used to generate Deepfakes, or 'Deepfake models', process existing performances by detecting and breaking down the input data into extremely fine data points to learn from and generate a new synthetic performance. The synthetic performance, or Deepfake, is able to imitate the input data without technically copying it, thanks to the deep learning performed by the AI systems.

Deepfake models detect patterns from the input data to separate data conveying the likeness of a performer or the likeness or style of a performance from the material it is interpreting (e.g. the speech, the dance routine and the song). These analyses are so minute that the AI is capable of separating the data points pertaining to each layer of the source material in ways the human eye or ear cannot.

The modelling process identifies the key markers relevant to each expressive layer embedded in the human performances (e.g. likeness, embodiment or interpretation versus the underlying movement or speech). The model can filter out markers, or data points, it does not seek to reproduce in the Deepfake. This results in the faithful synthetic imitation of a performer executing an entirely new, or different, speech or movement.

Most current Deepfake models use what are called a 'target' performance (executed by a target performer) and a 'driving' performance (executed by another performer, the driving performer). Both the 'target' and 'driving' performance are 'source' performances that the neural networks will learn from to generate the Deepfake. These source performances constitute the input data. The Deepfake constitutes the output data.

A 'target' performance is typically the performance from which the likeness of the performer and/or the interpretation is sought to be captured, reproduced and re-created in the synthetic performance. The 'driving' performance is typically used to manipulate the target performance so as to have it express new or different movements, expressions or sounds.

The Deepfake consists of synthetic data generated (or in AI terminology 'generalized') on the basis of performances by at least two performers (the target and driving performer). To what extent each of the source performances will influence the Deepfake depends on the desired effect and will be reflected in the design of the AI protocol.

In the example of the *Virtual Maggie* project (2018-present), film director and scholar Dominic Lees seeks to synthetise Margaret Thatcher to have her Deepfake feature in a period film (Lees, 2021). AI systems used to generate Thatcher's Deepfakes rely on recordings of her speeches and public appearances. Her synthetic avatar will be performing original dialogues and movement different from those featuring in the recordings of her 'authentic' performances. Thatcher's Deepfake will be driven by the performance of another actress cast for this purpose. The actress' driving performance is captured in a film, which will be processed by the AI system as 'source data', alongside the original recordings of Thatcher's 'real' speeches.

It is important to stress that AI systems create new data (the synthetic performances) resembling existing input data (the pre-existing performances). AI systems in this regard are not comparable to other forms of digital reproductions such as re-mixing or collages. Some models of AI systems for synthetisation will produce output performances that are entirely synthetic, others are designed to integrate synthetic content into authentic, 'real' footage with a view to replace or edit part of a performance (Pavis, 2020: 6). This discussion focuses its analysis on fully synthetic output content.

## Disruption

Synthetic performances or digital impersonations are not new and precede the emergence of Deepfakes. However, AI systems have introduced a step-change in the process of generating imitative synthetic performances, exemplified in Deepfakes (Whyte, 2020: 203–204; Yamaoka-Enkerlin, 2020: 729–730).

The technology used to generate Deepfakes, AI systems, is more accessible than any other technology capable of producing medium-to-high quality synthetic performances, like CGI or VFX. Deepfake technology is cheaper (requires less hardware or software to run), easier (requires fewer technical skills) and potentially quicker (depending on the input data used and output data desired) (Fletcher, 2018; Westerlund, 2019: 40–41; Caldera, 2019: 182–184; Lees, 2021). Unlike traditional methods, AI systems are also open source and available online. As AI technology develops, AI systems are soon expected to produce better results than traditional methods. Consequently, the making of high-quality or complex synthetic performances is no longer the preserve of well-resourced organisations or trained experts.

Another novel aspect of Deepfakes, enabled by AI systems, is their capacity to be produced from wide-ranging sources or formats of input data. Deepfakes can be made based on data captured from live performances, performance fixed in sound recording, and still or moving images. AI systems can also be trained to generate output synthetic data of a different format than that of the input data. For example, AI systems can be designed to generate (synthetic) moving images from still images.

## Primary stakeholders

In the context of a reflection on a balanced regulatory framework for Deepfakes, it is important to clearly define the key stakeholders involved in generating this type of content. This analysis identifies four key stakeholders:

1. the person(s) represented in the input data used to generate the Deepfake, the '*Deepfaked person(s)*';
2. the person(s) generating the Deepfake, 'the "*Deepfake maker(s)*"';
3. the person(s) receiving or viewing the Deepfake, the audience of '*Deepfake viewer(s)*'; and,
4. the person offering means to disseminate the Deepfake, such as distributors, online service providers or other intermediaries, the '*Deepfake disseminator(s)*'.

If we apply this typology of stakeholders to the example of *Virtual Maggie* introduced earlier, we obtain:

1. Margaret Thatcher and the actress driving the Deepfake as the 'Deepfaked persons';
2. Film director Lees and his creative team generating the Deepfake acting as 'Deepfake makers';
3. The audience of the film are the 'Deepfake viewers';
4. The film distributors or online service providers facilitating the public dissemination of the film as the 'Deepfake disseminator(s)'.

There may also be secondary stakeholders, which we define as individuals who do not directly come into contact with a Deepfake, but who may be affected by the actions or decisions of those who have. In the example of a Deepfake shared for the purpose of influencing elections, secondary

stakeholders will include any individual bound or affected by the results of the vote, who did not also come into contact with the Deepfake. The category of secondary stakeholders is thus broad and likely to evolve as applications of Deepfake technology expand. For this reason, the analysis focuses its principled approach on primary stakeholders.

## A principled approach for a balanced regulatory response to Deepfakes

This article proposes a principled approach to the regulation of Deepfakes which balances the interests of stakeholders and the applications of the technology. This approach responds to a tendency of law experts and legislators to focus on malicious uses of the technology to the detriment of other applications.

**Table 1.** Examples of recent reforms and proposals for reform targeting Deepfakes

| Jurisdictions | Status at the time of writing (March 2021) |
|---|---|
| Australia | |
| New South Wales | |
| Crimes Amendment (Intimate Images) Act (2017) No 29 | *Enacted* |
| Western Australia | |
| Criminal Law Amendment (Intimate Images) Act 2019 No 004 | *Enacted* |
| European Union | |
| European Commission (2021) Proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts. COM/2021/206 final | *Proposed* |
| France | |
| Law 2018-1202 (France). LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (2). JORF n°0297 du 23 décembre 2018, articles 6, 8 and 10 | *Enacted* |
| Electoral Code. Code électoral, Articles L163-1; L163-2 | *Enacted* |
| United States | |
| Federal level | |
| Malicious Deep Fake Prohibition Act of 2018 S.3805 | *Proposed* |
| Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019 (Accountability Act) H.R.3230 | *Proposed* |
| California | |
| Assembly Bill No 730, An act to amend, repeal, and add Section 35 of the Code of Civil Procedure, and to amend, add, and repeal Section 20010 of the Elections Code, relating to elections | |
| New York | |
| Senate Bill S5959D | *Enacted* |
| Assembly Bill A5605C | *Enacted* |
| Texas | |
| Election Code, s.255.004 | *Enacted* |

*(continued)*

**Table 1.** (continued)

| Jurisdictions | Status at the time of writing (March 2021) |
|---|---|
| Virginia | |
| Bill No 2678. A Bill to amend and reenact §18.2–386.2 of the Code of Virginia, relating to unlawful dissemination or sale of images of another; falsely created videographic or still image; penalty (Virginia) | *Enacted* |

Crimes Amendment (Intimate Images) Act 2017 No 29 (New South Wales) available at https://legislation.nsw.gov.au/#/view/act/2017/29/full

Criminal Law Amendment (Intimate Images) Act 2019 No 004 (Western Australia) available at https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_a147218.html

European Commission (2021) Proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts. COM/2021/206 final. Available at https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN. (accessed on 2 June 2021)

Law 2018-1202 (France). LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (2). JORF n°0297 du 23 décembre 2018. Available at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559

Electoral Code (France). Code electoral. Available at https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/2021-02-01/

Malicious Deep Fake Prohibition Act of 2018 S.3805. Available at https://www.congress.gov/bill/115th-congress/senate-bill/3805

Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019 (Accountability Act) H.R.3230. Available at https://www.congress.gov/bill/116th-congress/house-bill/3230

Assembly Bill No 730. An act to amend, repeal, and add Section 35 of the Code of Civil Procedure, and to amend, add, and repeal Section 20010 of the Elections Code, relating to elections. Available at https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201920200AB730

Senate Bill S5959D (New York) available at https://www.nysenate.gov/legislation/bills/2019/s5959

Assembly Bill A5605C (New York) available at https://www.nysenate.gov/legislation/bills/2019/a5605/amendment/c

Election Code (Texas) available at https://statutes.capitol.texas.gov/Docs/EL/htm/EL.255.htm#255.004

Bill No 2678. A Bill to Amend and Reenact §18.2-386.2 of the Code of Virginia, relating to unlawful dissemination or sale of images of another; falsely created videographic or still image; penalty (Virginia) Available at https://lis.virginia.gov/cgi-bin/legp604.exe?191+ful+HB2678S1+hil

This approach will be particularly relevant to jurisdictions where regulatory responses are under discussion by policy-makers but reforms have not yet taken place. This is the case of the UK and the European Union, for example (Pavis, 2020; UK Intellectual Property office, 2021, UK Law Commission, 2018; UK Intellectual Property Office, 2020; European Commission, 2021). In jurisdictions where reform has already occurred (Table 1), this principled approach can be used as a critical tool to measure effectiveness and assess the need for further reform.

## *Principles for a balanced regulatory response*

This analysis identifies three key principles to developing balanced regulatory responses to Deepfakes. Regulatory responses and policies must demonstrate:

1. an *accurate understanding of the technology* and the way in which it synthetises data (Principle 1);
2. the *capacity to account for negative (harmful) and positive (beneficial) applications* of the technology (Principle 2); and

3. a *clear definition of the primary stakeholders in Deepfakes combined with the balancing of their interests* (Principle 3).

The reform of performers' rights described in the section *A reform of performers' rights* implements these three principles.

## A benchmark of legal standards for the balanced regulation of Deepfakes

This section translates this principled approach into legal standards for the regulation of Deepfakes. This sub-section outlines these standards for each primary stakeholder in the context of positive and negative applications of Deepfake technology. Taken together, these legal standards form a benchmark to assess current and future reforms on Deepfakes. A balanced legal approach to the interests of each primary stakeholder would require providing for:

### *The Deepfaked person(s)*

(a) *The ability for individuals to prohibit certain Deepfakes* in which they are represented. This may take the form of a legal right to be free from harm caused by certain Deepfakes.
(b) *The ability for individuals to authorize commercial and non-commercial uses of certain Deepfakes* in which they are represented. This requires the legal right to consent to, or authorize Deepfakes, as well as the possibility to form secure contracts to that effect.
(c) *Access to effective remedies to support the control of certain Deepfakes* in which they are represented. Remedies are effective when: they involve no to low costs of enforcement; they can be quickly implemented; they take the appropriate form (e.g. damages, injunctions, content blocking or removal); they grant an appropriate level of compensation on account of all forms of recognized harm (economic, physical, psychological and moral or reputational harm); they are enforceable against the relevant primary stakeholders (e.g. Deepfake makers or Deepfake disseminators) and they are enforceable across jurisdictions (cross-border enforcement).
(d) These prerogatives would need to be *carefully balanced with the interests of the other primary stakeholders.* This may generate *obligations or duties* bearing on the Deepfaked person. An example of such obligation or duties may include the obligation or duty to respect the freedom of expression of other individuals generating Deepfakes – under certain circumstances.

### *The Deepfake maker*

(a) The *ability for individuals and organisations to generate Deepfakes.* This requires the formal recognition of a right to generate certain Deepfakes; the possibility to form secure contracts for the generation and dissemination of such Deepfakes.
(b) The *ability for individuals and organisations to authorize commercial and non-commercial uses of the Deepfakes that individuals have generated.* This may come in the form of a right in the nature of intellectual property or other. This will require the possibility to form secure contracts on the use and reuse of the Deepfakes they have generated.
(c) *Access to effective remedies to support the control over the Deepfakes individuals have generated.* See above for a description of what may constitute an effective remedy.
(d) Again, these prerogatives would need to be *balanced with the interests of the other primary stakeholders.* This may generate *obligations or duties* bearing on the Deepfake maker. For example, there may be limitations on an individual's right to generate a Deepfake rooted in

the right to privacy of the Deepfaked person(s). Similarly, the rights of the Deepfake viewer may override certain prerogatives of the Deepfake maker.

*The Deepfake viewer*

(a) The *ability for individuals to access, or engage with, certain Deepfakes.* This may require the recognition of a legal right to that effect.
(b) The *ability for individuals to detect certain Deepfakes before or immediately after viewing.* This may require the recognition of a legal right to that effect or as an obligation bearing on Deepfake makers or Deepfake disseminators.
(e) *Access to effective remedies to protect these prerogatives.* See above for a description of what may constitute an effective remedy.
(c) Again, these prerogatives would need to be *balanced with the interests of other primary stakeholders.* This may generate *obligations or duties* bearing on the Deepfake viewer. For example, one may imagine the creation of an obligation or duty for Deepfake viewers to report harmful Deepfakes in certain circumstances.

*The Deepfake disseminator*

(a) The *ability to disseminate certain Deepfakes, and control their dissemination.* This may require the formal recognition of a right to that effect as well as the possibility to form secure contracts.
(b) The *ability to determine Deepfakes appropriate for dissemination effectively.* This may come in the form of a clear definition of what constitutes a Deepfake appropriate for dissemination, and a clear account of Deepfake disseminators' liability in disseminating inappropriate Deepfakes.
(f) *Access to effective remedies to protect these prerogatives.* See above for a description of what may constitute an effective remedy.

Again, these prerogatives would need to be *balanced with the interests of other primary stakeholders*. This will likely generate *obligations or duties* bearing on the Deepfake disseminator similar to existing obligations resting on online service providers and content publishers in relation to intellectual property infringement, libel or children protection. For example, such obligations may involve the duty to take-down content following notification by a relevant party that infringing activity is taking place on the Deepfake disseminator's platform, or the duty to signal to Deepfakes viewers that they are accessing synthetic content.

## Gaps in knowledge

This article posits that the current state of scientific knowledge on Deepfakes is not sufficient to support the implementation of all aspects of this benchmark. At least two critical gaps have been noted by experts. The first is a gap in knowledge about positive or beneficial applications (pertinent to Principle 2). The second notes a gap in knowledge on the experience of Deepfake viewers (pertinent to Principle 3).

*Positive or beneficial applications.* Both the legal scholarship (e.g. Chesney and Citron, 2019b; Delfino, 2020; Franks and Waldman, 2019; Ice, 2019; James, 2020; O'Connell, 2020; Pechenik Gieseke, 2020) and recent legislative efforts have tended to focus on malicious Deepfakes (e.g. Table 1).

This is also true of the UK where the government commissioned a review of the law on online sexual abuse or image-based abuse which included Deepfakes (Law Commission, 2018). By contrast, Deepfakes were left out of the scope of a subsequent government review assessing the need to reform the UK intellectual property framework in light of AI technology (Pavis, 2020; UK Intellectual Property Office, 2020). The first review includes Deepfakes for the purpose of sanction, whereas they are excluded from a discussion focused on supporting innovation in the second.

There are two exceptions to this over-focus on malicious applications of Deepfakes in global policy-making which should be noted. The first is the reform of privacy and publicity rights in the state of New York (US), as the scope of these rights would cover consensual and non-consensual uses of the technology (Assembly Bill AA5605C; Senate Bill S5959D). The second is the very recent proposal by the European Commission published in April 2021. This proposal does not frame Deepfakes as harmful so long as the manipulation of input data is clearly communicated (European Commission, 2021: 5.2.4, Art.52).

A cause or consequence of this over-focus on malicious applications is a lack of critical reflection and empirical evidence regarding positive or beneficial uses of Deepfakes. This leads to a gap in the knowledge of what may constitute an appropriate, justified or legitimate Deepfake. Similarly, stakeholders' interests in generating and distributing this type of Deepfake are not yet well understood.

This over-focus on malicious applications creates an oversight of legitimate uses of Deepfakes in policy-making (Pavis, 2020). This article contributes to bridging this gap by putting forward a regulatory tool (performers' rights) capable of regulating certain positive applications of Deepfake technology.

*The Deepfake viewer.* At present, the role of the viewer, the audience or the 'networked public' in realizing the harms and benefits of Deepfakes remains under-explored (Bode, 2021; Ekaratne, 2020: 355). The 'viewer' of Deepfakes requires further interdisciplinary research and critical analysis by scholars and integrating into regulatory measures by law-makers (Bode, 2021; Helm and Nasu, 2021). As argued by Bode (2021) in her seminal work on the topic, viewers' reception of Deepfakes is nuanced, complex and very subtly affected by context or the individuals' own background knowledge on the content to which they are exposed.

To date, legal responses and analyses have tended to focus on defining the behaviour of the wrongdoer (the person(s) making the Deepfakes) and the person(s) harmed by the Deepfakes (the person represented in the Deepfake). Viewers, and their reception of Deepfakes, have been overlooked in this assessment.

This criticism was raised by Helm and Nasu (2021) in relation to anti-fake news regulation and can be repeated in the context of Deepfakes reforms. Helm and Nasu stress the need for anti-fake news regulation to engage with empirical evidence on the viewer's reception of manipulated content to be effective.

Where the impact of Deepfakes on the viewer was central to legal reforms, as it is the case of anti-fake news regulation or amendments to electoral laws, these measures were introduced on the basis of assumed or presumed reception by viewers without consideration for established empirical evidence from scientific studies on information disorder (Helm and Nasu, 2021) and audiences' reception of fiction and non-fiction content (Bode, 2021).

Similarly, there has been no critical or legal doctrinal analysis performed on the rights and liabilities of Deepfakes viewers when engaging with Deepfakes. Again, the proposal by the European Commission may be the one exception. The text recommends the introduction of transparency obligations for 'providers' of Deepfakes to empower the viewer in making 'informed choices or step back from a given situation' (European Commission, 2021: para.5.2.4).

Noting both of these gaps in knowledge, this article chooses to focus on developing regulatory solutions for positive and negative applications of Deepfake technology in relation to the better understood aspect of the benchmark: the Deepfaked person(s).

## Existing standard of protection for the Deepfaked person

This section reviews the laws of England and Wales against the benchmark with a focus on the interests of the Deepfaked person. In doing so, it identifies seven main limitations in the standard of protection available to this primary stakeholder, which can be overcome with a reform in performers' rights as argued below (*Raising standards of protection for the Deepfaked person: a solution in performers' rights* and *A reform of performers' rights*).

A note on language and references before turning to this review. The following discussion uses the term 'legal remedies' to refer to legal provisions, causes of actions or other forms of judicial relief enforcing legal rights recognized in law, and enforceable by a court or a public body, regardless of their criminal or civil nature.

As for references, the primary sources of law relevant to this analysis feature in footnotes to ease reading. References to leading or recent commentary by law specialists on the practical application of these remedies are indicated in the text as an alternative, more accessible, source for readers. Where available, commentary specific to Deepfakes is given precedence. This simplified approach to language and references speaks to the need for developing legal analysis on Deepfakes accessible to non-lawyers.

### *Existing legal remedies for the protection of Deepfaked persons in England and Wales*

In England and Wales, the key remedies relevant to regulating Deepfakes amount to no less than 13 civil causes of action and criminal offenses (Farish, 2020a, 2020b; O'Connell, 2020; Perot and Mostert, 2020).[2] Despite this range, this analysis demonstrates that none provide sufficient protection for the Deepfaked person's interests.

These legal remedies include: the *right to privacy*[3] also known as the tort of misuse of private information (Farish, 2020a; Gomery, 2007; O'Connell, 2020); *the tort of breach of confidence*[4] (Deazley, 2003; Farish, 2020b); the *tort of passing off*[5] (Oke, 2020; Tan, 2017); the *tort of defamation*[6] (Farish, 2020b; Waever, 2020); the *tort of malicious falsehood* (Farish, 2020b; Smith, 2020); *copyright*[7] (O'Connell, 2020; O'Connell and Bakina, 2020; Perrot and Mostert, 2020); *performers' rights*[8] (Farish, 2020b; Pavis, 2020, 2021a, 2021b); remedies under *data protection regulation*[9] (Farish, 2020b); civil and criminal remedies against *harassment*[10] (Bliss, 2019; Farish, 2020b); *private sexual image regulation*[11] (O'Connell, 2020); *communications offences*[12] (Farish, 2020b; Greenberg, 2021); *offences for the misuse of computers*[13] (Farish, 2020b; Montasari et al., 2016).

### *Limitations of existing remedies for the protection of Deepfaked persons*

These remedies are assessed against the standards safeguarding the Deepfaked person's interests, as outlined above.

*Limitation 1 – post-mortem use of source data.* Existing legal remedies do not apply well, or at all, to unauthorized uses of data after the death of the person represented in the data, that is, use of data post-mortem (Edwards and Harbinja, 2013; Gibson, 2020; Harbinja, 2017). This limitation has affected the application of the *right of privacy, malicious falsehood and defamation*. These remedies would be ineffectual in regulating unauthorized Deepfakes using data post-mortem.

*Limitation 2 – use of public source data and source data about public figures.* Existing legal remedies do not apply well, or sometimes at all, to unauthorized uses of data that was previously made public lawfully, or that relates to public figures (Campbell, 2020; Farish, 2020a; Gomery, 2007; O'Connell, 2020: 19–20). Unauthorized uses, or reuses, of such data have limited the application of the *right of privacy* and *breach of confidence* in the past. These remedies would be ineffectual in regulating unauthorized Deepfakes that were generated using public data or data about public figures.

*Limitation 3 – use of data about unknown (private) individuals.* Claims seeking to control individuals' reputation or goodwill will be limited for those who cannot prove they enjoy such reputation or goodwill in the first place, such unknown or private individuals or anyone not able to evidence the extent of their reputation (Carty, 2012; Oke, 2020; Tan, 2017; Wragg, 2020). This limitation affects claims of *passing off* primarily, which will be less effective in regulating Deepfakes made using data related to a private person.

*Limitation 4 – use of data by unknown or anonymous individuals.* The vast majority of claims or legal proceedings will be limited, or defeated, against defendants that are unknown to the claimant for their identity or whose acts have remained anonymous. This is the case for many forms of online publications. This also affects any legal remedies exclusively directed at the wrongdoer, rather than third parties involved in, or participating in the incident causing harm such as individuals or organisation re-using, re-uploading or hosting unauthorized Deepfakes created by someone else (O'Connell, 2020).

Use of data by unknown or anonymous individuals, limit all the listed legal remedies except two: *copyright* and *defamation*. Defamation and copyright laws provide take-down notifications which can be issued against internet platforms, hosts or publishers to withdraw materials alleged to be infringing upon the rightsholder's copyright.[14] Online platforms are required to take-down content upon notice by the person represented in the data (O'Connell, 2020: 58–59; Coors, 2015: 75).

*Limitation 5 – use of data that does not lead to 'serious harm' or quantifiable economic harm.* Another limitation of existing legal remedies is their focus on 'serious harm' (*defamation*, Rudkin, 2014) or quantifiable economic harm (*malicious falsehood*, Smith, 2020; *passing off*, Wadlow, 2016). This limits the application of certain remedies to cases where authorized used of data, via Deepfakes or other means, does not lead to what a court would regard as 'serious harm' or quantifiable economic damage. Damages for pain and suffering, notably psychological harm such as distress are also recognized, but the amount awarded tends to be substantially lower than in the context of quantifiable economic harm that can be evidenced by the claimant.[15] This limits the effectiveness of the *right of privacy* and *breach of confidence* (Saied, 2020).

*Limitation 6 – use of data representing someone else than the owner of the data.* Ownership of data does not always belong to the person represented in it. For example, content may be owned by intellectual property rights that do not belong to the person represented in, or whose face, voice, likeness or performance features in the data. A typical example of this limitation is *copyright*. Most material created for the purpose of online publications, or content distribution broadly understood, are eligible for copyright protection. But there are rare instances where the copyright in the materials is owned by the person featuring in it (Gibson, 2020; O'Connell, 2020; Pavis, 2018). For example, an article relating a person's biography will belong to the author of the text, rather than the person reflected in the text. The photograph of an individual will place right to copyright in the hands of the photographer rather than the person being photographed.

*Limitation 7 – international or cross-border use of data.* Existing legal remedies do not apply well, or at all, to unauthorized uses of data outside the jurisdiction of the person represented in the data, or in jurisdictions with lower levels of protection (Gibson, 2020). This limitation is particularly problematic for online communications as these activities can easily occur cross-border. The absence of international harmonisation of the legal remedies makes cross-border judicial proceedings difficult. This limitation affects all of the listed legal remedies except *copyright* and *performers' rights*. Both rights have received a degree of international harmonisation.[16] *Data protection regulations* are also harmonised at the regional level of the European Union.[17]

## Raising standards of protection for the Deepfaked person: a solution in performers' rights

This article proposes performers' rights as a more sophisticated legal response to Deepfakes than existing legal remedies, because their regime would raise the standards of protection granted to Deepfaked persons. This section describes this regime to demonstrate the contribution performers' rights can make to re-balancing the regulation of Deepfakes if adequately reformed.

### *Description of performers' rights*

Performers' rights are a type of intellectual property rights. Performers' rights, as their name indicates, protect the economic and moral rights interests of 'performers' in making and selling recordings of their work (the performances). Performers' rights are similar to, but should not be confused with, copyright.

*Protected 'performances' and 'performers'.* Performers' rights have a wide scope of application because the definition of a 'protected performance' or a 'protected performer' in the meaning of intellectual property law has been written in broad terms by national (UK) and international legislators (Pavis, 2018, 2020).[18]

The law classes as protected 'performance' for the purpose of performers' rights anyone who speaks sings, dances or simply moves with the intention to convey dramatic meaning (understood broadly) (Arnold, 2016; Pavis, 2018, 2019: 63, 149). Such a 'performance' can be live or fixed in a recording. This definition includes improvisations, spontaneous expressions as well as rehearsed content.

Importantly, the law makes no reference to notions of originality, quality, aesthetic merit, professional or amateur status in defining protected performances or performers. Similarly, there is no requirement based on the performer's reputation, notoriety, professional or amateur status, or goodwill to receive protection under performers' rights.

Under this definition, teachers, politicians, journalists as well as individuals sharing their videos on social media are 'performers' legally entitled to control the records made of their 'performances' (Pavis, 2018, 2019). As a result, the use of these recordings as input data to generate a Deepfake would fall within the scope of performers' rights granting protection to the target and driving individual (if adequately reformed) (Pavis, 2020).

In this regard, the scope of application of performers' rights is more flexible than most other legal remedies, and addresses Limitations 2 and 4.

*Consent and control over the 'performances'.* Performers' rights give performers control over their performance, whether it is live or recorded.[19] This control is two-fold as it manifests in the legal right

to consent to the fixation of their performances in recordings (in sound recordings or films) on the one hand, and the legal right to consent to the subsequent use of these recordings on the other hand.[20]

Consequently, and with the appropriate reform, performers' rights would apply to any form of input data capturing an individual's performance whether they are the target or driving performance. Similarly, performers' rights would also apply regardless of whether the input performances synthesised by AI systems are live or in still photographs, sound recordings or films (Pavis, 2020).

Performers' rights also include moral rights that guarantee that their work is treated with respect, or in accordance with industry standards, and that performers are acknowledged for their contribution to a performance or larger productions.[21]

The law regards the act of recording (or fixing) a performance and use of that recording as separate activities, each requiring the consent of the performer. In practice this means that a performer must consent to the fixation of their performance in a recording, and to the use of these recordings separately. For example, an actor or a musician must authorize the recording of their performance in the studio. Their consent is also required for the producer to release that recording to the public. Similarly, such consent would also be required if these recordings were being used for the purpose of synthetisation, following the reform recommended below in the section *A reform of performers' rights*.

Consenting to the recording of a performance and to the subsequent use of that recording is managed via contracts, under conditions provided by the law. Extending the application of performers' rights to Deepfakes allows Deepfaked persons, Deepfake makers and disseminators to form legally secure contracts for the making and dissemination of legitimate Deepfakes. This will also allow Deepfaked persons to benefit from the commercialisation of Deepfakes representing them, where appropriate.

It is technically possible to consent to the synthetisation of one's performance by contract, without the existence of recognized intellectual property rights like performers' rights. This was illustrated by the *Rooney* Case [22] in which a professional footballer commercialized his image through contract despite the fact that image rights do not exist in England and Wales. This practice is, however, less secure, and will give rise to lower, or uncertain, levels of damages in cases of infringement.[23] It is also only available to individuals with high to very high contractual bargaining power.

The ownership of performers' rights first belongs to the performance, that is, the individual represented in the performance. As such performers' rights would resolve *Limitation 6.*

*Remedies.* As an intellectual property right, performers' rights give access to civil remedies enforceable in court by the rightsholder (the performer, or the person in the Deepfake). Remedies may come in the form of an injunction (i.e. an order of the court to withdraw content or refrain from publishing the content) or damages (i.e. financial compensation for the economic loss suffered by the making and dissemination of the Deepfakes). That performers' rights include moral rights allows for the financial compensations of reputational or moral prejudice in the treatment of the performance in the Deepfake, as well as economic prejudice, thereby bridging Limitation 6.

Whilst those remedies are comprehensive, they require initiating legal proceedings which can be costly. Civil legal proceedings also necessitate knowing the identity of the right infringer which, as per Limitation 5, will not always be the case, notably in the context of anonymous online abuse. This limitation affects the current regime of performers' rights but is mitigated by the proposals for reform outlined in the section *Raising standards of protection for the Deepfaked person: a solution in performers' rights*.

Considering the online dissemination of Deepfakes, take-down notices can be a valuable remedy fit for the harm at play. This remedy can be a tool to involve platforms in governance of Deepfakes.

However, this approach is not without criticism, as platforms tend to be over-zealous in withdrawing content to avoid liability both in the context of copyright infringement (Blythe, 2019; Garstka and Polanski, 2019) and speech regulation (Schwiddesssen et al., 2018).

*Duration of protection.* Performers' rights last at least for a period of 50 years starting form the end of the year the performance occurred or was published. The rights can survive the death of the performer,[24] and be managed by their heirs to control post-mortem uses (addressing Limitation 1).[25]

*Exceptions to protection by performers' rights.* Like copyright, performers' rights provide for a series of 'exceptions' and 'limitations' to protection in cases to allow uses of protected performances without the consent of the rightsholder (the performer) (Arnold, 2016: 288–231).[26] These 'exceptions' and 'limitations' aim to balance the protection given to performers with the interests of other stakeholders such as producers, distributors and the public who may want to reuse performances in ways which are consistent with their right to free speech and creative expression.

*International harmonisation.* Like copyright, performers' rights have received international recognition in a series of conventions and treaties and have been harmonized in this process.[27] Consequently, performers' rights are a common, and harmonised feature, for a large number of jurisdictions. As such, they can offer a meaningful response to cross-border issues like those posed by Deepfakes by providing a legal basis for a global regulatory response to Deepfakes by the international community. This is an advantage performers' rights hold over regulatory solutions based on image rights or personality rights for which there is no existing framework of international harmonisation for the international community of policy-makers to build on.

This international harmonisation enables parties to form secure contracts between jurisdictions providing the similar level of protection under performers' rights. It will facilitate the enforcement of performers' rights in the event of infringement in another, or multiple, jurisdictions where the level of protection is harmonized. This aspect of performers' rights also addresses Limitation 7.

## *Performers' rights applied to Deepfakes: an illustration*

If performers' rights applied in the case of *Virtual Maggie* by Lees, the performances of two individuals would be subject to performers' rights (if these were to be reformed accordingly). The first is Margaret Thatcher herself, for the performances captured in the recordings used by the AI systems to generate her digital avatar. The second is the actress driving Thatcher's digital avatar. In this context, the Deepfake generated under Lees' direction holds two sets of performers' rights, one belonging to Margaret Thatcher's estate and another belonging to the actress. Lees would need to secure the consent of each rightsholder (Thatcher's estate and the actress) to use each of their performances to generate Thatcher's Deepfake. This would be done through a contractual agreement to that effect. A full transfer of rights from the performers to Lees would need to be recorded in writing and be signed by the performers, giving them both the opportunity to negotiate suitable terms and remuneration.

It is also possible to conceive Thatcher's Deepfake as a third protected performance subject to its own set of performers' rights – should performers' rights be reformed in this regard (Pavis, 2020; UKIPO, 2020). If so, it is expected that the performers' rights vested in the (new) digital performance (the Deepfake) was jointly owned by both Thatcher's estate and the actress. Both of their consent would be required for the subsequent use of the Deepfake, by Lees or other third parties. It is both possible and plausible that Lees and/or his creative team would have made a substantial creative contribution to the

rendering of the new digital performance (the Deepfake) due to the collaborative nature of the making process. If so, it is legally conceivable to reflect the collaborative nature of the process in the distribution of rights by listing Lees and/or his creative team as joint-owners (McDonagh, 2021; Simone, 2019). All of the above requires a reform of performers' rights as outlined in the section *A reform of performers' rights*.

### *Assessment of performers' rights against the benchmark*

Performers' rights address the seven limitations faced by existing legal remedies. As such performers' rights fairs significantly better than existing remedies in achieving the standard of protection set by our benchmark.

The benchmark required that individuals (protected performers) receive:

(a) *the ability to prohibit and sanction certain Deepfakes*, which performers' rights confer in the form of property and non-property rights to consent to the fixation of performances and the subsequent use of these recordings.
(b) *the ability to authorize and control certain Deepfakes for commercial and non-commercial uses*, which performers' rights provide by granting intellectual property rights transferrable via a secure contract. The international harmonisation of performers' rights offers the possibility of forming cross-border contracts.
(c) *access to effective remedies*, which performers' rights provide to the extent that they give access to damages, injunctions as well as take-down notices against certain Deepfake disseminators (if adequately reformed). Remedies would account for both economic and moral interests to the extent that the regime of protection includes economic and moral rights. Performers' rights' international harmonisation also offers a degree of cross-border enforcement of rights.
(d) legal protection *balanced with the interests of other primary stakeholders*; performers' rights make provision for such balancing of interests in its provisions for exceptions to protection.

At this stage, two aspects in the standard of protection provided by performers' rights for the Deepfaked person could be improved, separate from the reform proposed below.

The first relates to improving the effectiveness of remedies. Performers' rights are civil remedies and require active engagement by the rightsholder (the Deepfaked persons) with legal proceedings. These remedies rely on the Deepfake persons' financial resources and legal knowledge to engage with such proceedings. This obstacle could be mitigated by the introduction of complementary support allowing a third party such as the state (via prosecution) or other organisations (such as Deepfake disseminators, a regulatory body or representative organisations) to take actions on behalf of Deepfaked persons or in defence of their interests. This can be achieved via a reform of criminal legislation or the introduction of ad hoc regulations to that effect. For this reason, it is argued that the benchmark for the protection of Deepfake persons' interests is more likely to be met through a regulatory response combining a reform of performers' rights and a reform of criminal legislation, or an equivalent.

The second regards the exceptions to performers' rights protection provided by statutory law. These exceptions are fundamental to the balancing of stakeholders' interests vested in intellectual property framework, and as such they are core to this area of law. Similar exceptions are found in copyright law, and to an extent patent law. However, exceptions to protection in copyright and

patent law have been criticized by law experts for being too narrow, and not sufficient in providing an effective balance of interests between stakeholders and the public (i.e. users of the technology protected by the law) (Deazley, 2017; Jacques, 2019; Walsh et al., 2021). These criticisms would apply to the current regime of performers' rights, limiting its performance on this aspect of the benchmark. Consequently, a reform of performers' rights may require a revision of current exceptions to protection to better account for the interests of other primary stakeholders in Deepfakes (Pavis, 2020: 13).

Setting these caveats aside, performers' rights perform well against this benchmark – no pun intended. However, this result can only be achieved if performers' rights are reformed. This is because Deepfakes and Deepfake technology falls outside the scope of protection conferred by performers' rights at present.

## A reform of performers' rights

In making its case for performers' rights as a suitable regulatory response to Deepfakes, this article uncovers a tension: whilst performers' rights are an attractive solution to regulate Deepfakes, this technology also challenges their scope of application. This is because Deepfakes uses content protected by performers' rights (performances) in a way unforeseen by intellectual property policy-makers at the time these rights were introduced into law. In order for performers' rights to live up to the benchmark described in the section *A principled approach for a balanced regulatory response to Deepfakes*, they require reform.

A reform of performers' rights will ensure this proposal complies with *Principle 1*, *2* and *3* of the approach to policy-making on Deepfakes proposed as a starting point of this analysis.

### *The gap in performers' rights*

Performers' rights currently protect the recording of a performance and the reproductions (or copies) of that recording. Performers can only control the fixed, recorded, version of their performance. By contrast, the content of the recording, the performance, is not protected and can be re-performed and imitated without consequences under performers' rights. This legal detail has significant implications in practice because it means that a performer has no (intellectual property) right to the substance or style of their performance (Arnold, 2016: 149).

Deepfakes challenge the framework of performers' rights insofar as it is capable of reproducing performances without generating a 'recording' or a 'copy' of a recording. In the strictest sense, AI systems used to generate Deepfakes do not record performances or copy recordings of performances, as explained in the section *Definition and description of Deepfakes*. Deepfakes reproduce performances without reproducing the recordings of those performances. As such, Deepfakes fall outside the scope of protection afforded by performers' rights.

We return to our digital impersonation of Thatcher to clarify this point. Performances delivered by Thatcher in her public speeches are eligible for protection by performers' rights and are available to us today in recorded form. If anyone makes a copy of these recordings, this would be an act of infringement of Thatcher's performer's rights. The same applies if someone had recorded Thatcher without her consent. However, the re-performance of Thatcher's speeches by actors who closely imitate her appearance, her voice and her style of interpretation, does not. Neither does the synthetisation of Thatcher's performances using AI systems. This is because, like the actors, AI systems are capable of producing a digital imitation of a performance without physically copying the recordings.

It is a little-known but key feature of performers' rights that the protection attaches to the recording of the performance, and its subsequent use, rather than to the performance contained within the recording. This limitation on the legal protection conferred by performers' rights is not new, and has been a feature of performers' rights since their introduction at the international and national level in 1961 and 1988 for the UK.[28]

It is an essential difference between the regime of copyright (which would extend to the style and substance of the performance if it applied) and performers' rights. The intention behind this limitation of performers' rights' regime is somewhat muddy. One the one hand, it can be explained by the intention of international and national legislators to create a clear demarcation between copyright and performers' rights (Arnold, 2016: 8–13; Pavis, 2016a, 2016b). Performers were to receive a differentiated legal protection, lesser than that of authors. This questionable intention was written into the regime of performers' rights in various places, including but not limited to the right of reproduction (Pavis, 2016a, 2016b).

On the other hand, it also appears that legislators did not anticipate the technological changes introduced by AI systems, necessitating augmented protection today. At the time performers' rights were introduced, giving performers a legal right to control the substance of their performance would have only served to regulate re-performances by humans like look-alikes and sound-alikes. These were not regarded as threats serious enough to justify protection. It is argued that this status quo has changed with the application of AI systems to the synthetisation of performances, as exemplified by Deepfakes.

There is precedent for step-changes in the legal protection of performers to be triggered by technological developments. The UK and other jurisdictions introduced legal provisions to protect performers' economic interest against the development of sound recording and films which allowed for the illegal bootlegging of performances in a way that could not be contained without legal rights (Arnold, 2016: 17–18). These national measures were then recognized by international law.[29]

## *Options for reform of performers' rights*

There are two routes for the reform of performers' rights in response to Deepfakes. The first is an ad hoc amendment of existing legislative provisions. The second, and recommended option, involves migrating the regime of performers' rights into the scope of copyright protection.

*Amending performers' rights (Option 1).* National and international law could be amended to include the making of Deepfakes within the scope of activities controlled by performers' rights. This amendment would require a modification of the statutory provisions defining the right to record a performance, and the right to make copies of these recordings to ensure that it covers reproduction of the performance itself, or at least references reproduction of performances via synthetisation (Pavis, 2020: 13–25).

In the UK, such modifications would have to be made to Sections 182 and Sections 182A of the CDPA, 1988. Under international law, equivalent modifications would have to be made to corresponding provisions, those being Articles 3 and/or Article 7 of the Rome Convention, and Articles 2, 6 and 7 of both the WPPT, 1996 and the Beijing Treaty (2012).

Alternatively, a similar outcome can be achieved by introducing a third, stand-alone, economic right to control or consent to the reproduction of the performance, at the national or international level (Pavis, 2020: 13–25).

This modification of the regime of performers' rights would bring the performer's legal protection closer to what authors receive under copyright, for which the right to control all forms of

reproduction of the work already exist (Griffiths, 2013: 768–775; Pihlajarinne, 2017).[30] However, the two sets of rights would remain different on other aspects of their regimes such as duration or accessory liability.[31] For these reasons, the second proposal of reform described below is preferred.

*Creating a performers' copyright (Option 2).* National and international law could be reformed in order to extend copyright protection to performers; in effect, replacing existing performers' rights with a performers' *copyright*.

This reform can be achieved by adding current beneficiaries of performers' rights to the list of individuals eligible for copyright protection. Under UK law, eligibility for copyright protection is determined with reference to the work, in our case the 'performance', provided that certain requirements are met such as categorisation, fixation, originality, not excluded on the grounds of public policy, and link to the UK.[32]

The thrust of reform is relatively straightforward. It entails adding the word 'performance', and the appropriate definition for that word, to the list of copyright protected works. 'Performance' would also have to be referenced under Section 1(1) of the CDPA, and in a new separate section between Section 3A and Section 9 of the Act that would give a definition of 'performance' in this context.

Other minor modifications of the text may also be necessary in order to maintain the internal coherence of subsequent provisions detailing the regime of protection of copyright, no least in relation to equitable remuneration rights. Under international law, this reform may necessitate the introduction of a new international convention for it is a significant departure from our current nomenclature of intellectual property rights.

This reform of performer's protection would have a number of valuable implications in addition to the benefits already indicated above. For example, the length of duration of the rights would be extended to the lifetime of the performer, plus 70 years, offering longer protection against inappropriate post-mortem Deepfakes.[33] The reform will also give access to notices and take-downs described in the section *Existing standards of protection for the Deepfaked person*.

With the introduction of a performers' copyright, performers' rights may be redundant. For this reason, performers' rights should be removed from national laws, where a stronger alternative form of protection has been provided.

## Challenges of the reform

There are two key challenges to the reform of performers' rights proposed in this reform. The first is that it would implement a step-change in intellectual property policy-making. The second regards the unintended negative effects that granting transferable rights over someone's likeness (as captured in a performance) may have on the protection of Deepfaked persons *in practice*.

*A step-change in intellectual property policy-making.* Introducing a performers' copyright represents a significant step-change from the standpoint of intellectual property policy-making. This reform would have the effect of redefining the taxonomy of rights separating authors' rights (copyright) from performers' rights (Pavis, 2016b). The second option, especially, substantially reshapes the landscape of intellectual property as we have known it for as long as performers' rights have existed.

This reshaping of intellectual property law is justified for several reasons. First, this reform would offer a comprehensive and more sustainable legal response to Deepfakes. Second, it would simplify the structure of intellectual property by removing a sub-category of intellectual property right

(performers' rights) and integrating it into the more-established regime of copyright. Third, this reform modernizes the intellectual framework by removing the archaic divide placed between authors and performers, which has no legitimate justifications today (Pavis, 2016a, 2016b).

*Unintended consequences of creating transferable rights in the nature of property.* This reform of performers' rights will have the effect of creating transferable property rights over the performance and likeness of the Deepfaked persons. A similar development of publicity rights took place in the US (Rothman, 2018: 45–113). Rothman points to the unintended, perverse, effect of this transformation of the publicity right from a (non-transferable) right grounded in the protection of individuals' privacy to a transferable property right rooted in individuals' publicity and logics of intellectual property. She explains that this mutation lowered the standard of protection conferred to individuals, whom she calls 'identity-holders' (the Deepfaked persons in our analysis) in *practice*. This is because the transferable nature of publicity rights led to a loss of control by identity-holders over their identity where and when they lacked the bargaining power, financial resources or legal knowledge to negotiate equitable contractual terms with producers or distributors who acquired the rights (Rothman, 2018: 115–137). The proposed reform of performers' rights could lead to similar results if suitable safeguards are not included, such as preventing or limiting the complete transfer of rights to third parties (Rothman, 2018: 115–137; Pavis, 2021b).

## Conclusion

This article proposed a principled approach and benchmark for the formulation and review of regulatory responses to Deepfakes. The analysis applied these tools to measure the standard of protection given to individuals represented in Deepfakes by existing legal remedies in England and Wales. This analysis reveals that performers' rights fair better against the benchmark of protection than existing legal remedies, and should be considered as a suitable route for reform in the regulation of Deepfakes. However, performers' rights do require reform to achieve this outcome. This article argued that optimal results would be obtained by creating a performers' copyright combined with a modification of criminal legislation. As regards performers' rights, such a reform would serve to simplify and modernise the framework of intellectual property.

### Acknowledgement

I am grateful to the editors of this special edition for their patience. I am indebted to Drs Dimitri Kagiaros, Karen Walsh, Naomi Hawkins and Timon Hugh-Davies for their invaluable comments on earlier version of this article. Mistakes or errors are my own. Time of writing: March 2021. Last editing: May 2021.

### ORCID iD

Mathilde Pavis https://orcid.org/0000-0002-1251-8398

### Notes

1. This article draws on conclusions submitted to the UK government in November 2020, in response to their call for views on AI and Intellectual Property Law ((UK Intellectual Property Office (2020), Artificial Intelligence and Intellectual Property: A Call for Views (Published 7 September 2020). Available at: https://www.gov.uk/government/consultations/artificial-intelligence-and-intellectual-property-call-for-views accessed on 16 March 2021); (Submission to the UK IPO: artificial intelligence and performers'

rights. pp. 1–28. DOI: 10.5281/zenodo.4298854. Available at: https://zenodo.org/record/4298855#.YE_)) and applies this analysis to Deepfakes specifically.

2. The analysis counts civil and criminal harassment claims as two separate remedies.
3. Human Right Act 1988 (Human Right Act 1998, c. 42 available athttps://www.legislation.gov.uk/ukpga/1998/42/contents); Goodwin (2011) (Goodwin v News Groups Newspapers Ltd [2011] EWCH 1437 (QB)); Campbell (2004) (Campbell v MGN [2004] UKHL 22).
4. (Coco v A. N. Clark (Engineers) Ltd [1969] RPC 41)
5. (Irvine v Talksport [2003] EWCA Civ 423)
6. (Defamation Act 2013, c. 26 available at https://www.legislation.gov.uk/ukpga/2013/26/contents/enacted); Sim (1936) (Sim v Stretch [1936] 2 All ER 1237)
7. Copyright, Designs, and Patent Act 1988, c 48 available at https://www.legislation.gov.uk/ukpga/1988/48/contents
8. CDPA
9. The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (Retained Regulations 2019) No 419 available at https://www.legislation.gov.uk/uksi/2019/419/contents/made; Data Protection Act 2018, c. 12 available at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
10. Protection from Harassment Act 1997, c. 40 available at https://www.legislation.gov.uk/ukpga/1997/40/contents); Majrowski (2005) (Majrowski v Guys and St Thomas's NHS Trust [2005] EWCA Civ 251
11. Criminal Justice and Courts Act 2015, c. 2 available at https://www.legislation.gov.uk/ukpga/2015/2/contents/enacted
12. Malicious Communications Act 1988, c. 27 available at https://www.legislation.gov.uk/ukpga/1988/27/contents; Communications Act 2003, c. 21 available at https://www.legislation.gov.uk/ukpga/2003/21/section/127; Chambers v DPP [2012] EWCH 2157 (Admin); R (Chabloz v CPS [2019] EWHC 3094 (Admin)
13. Computer Misuse Act 1990, c. 18, available at https://www.legislation.gov.uk/ukpga/1990/18/contents
14. The Electronic Commerce (EC Directive) Regulations 2002 No 2013 available at https://www.legislation.gov.uk/uksi/2002/2013/contents/made, s.19, s.13, s.22; Defamation Act 2013, s.5 and s.10.
15. Mosley (2008), para 219-223, 236 (Mosley v News Group Newspaper Ltd [2008] EWHC 1777 (QB)).
16. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) 1994. Available at https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm); Berne Convention for the Protection of Literary and Artistic Works (Berne Convention) 1886. Availablet https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm; Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention 1961. Available at https://www.wipo.int/treaties/en/ip/rome/); WIPO Performances and Phonograms Treaty (WPPT) 1996. Available at https://www.wipo.int/treaties/en/ip/wppt/; Beijing Treaty on Audiovisual Performances (Beijing Treaty) 2012. Available at https://www.wipo.int/treaties/en/ip/beijing/.
17. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, 1–88.
18. Copyright, Designs, and Patent Act 1988, c 48 available at https://www.legislation.gov.uk/ukpga/1988/48/contents; Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention) 1961. Available at https://www.wipo.int/treaties/en/ip/rome/; WIPO Performances and Phonograms Treaty (WPPT) 1996. Available at https://www.wipo.int/treaties/en/ip/wppt/, Article 2(a); Beijing, Article 2(a).
19. CDPA, Part II.
20. CDPA, s.182, s.182A-184.

21. (CDPA, s.205C, s.205F.
22. Proactive Sports Management Ltd v Rooney [2011] EWCA Civ 1444
23. See for example, Morris (2018) para 93-94 (Morris Garner v One Step Support Ltd [2018] UKSC 20).
24. CDPA, s.191.
25. CDPA, s.191B(1).
26. CDPA s.189, s.205E, s.205G
27. Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention) 1961. Available at https://www.wipo.int/treaties/en/ip/rome/, WIPO Performances and Phonograms Treaty (WPPT) 1996. Available at https://www.wipo.int/treaties/en/ip/wppt/, Beijing Treaty on Audiovisual Performances (Beijing Treaty) 2012. Available at https://www.wipo.int/treaties/en/ip/beijing/, TRIPS 1994.
28. Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention) 1961. Available at https://www.wipo.int/treaties/en/ip/rome/; CDPA.
29. Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention) 1961. Available at https://www.wipo.int/treaties/en/ip/rome/; WIPO Performances and Phonograms Treaty (WPPT) 1996. Available at https://www.wipo.int/treaties/en/ip/wppt/; Beijing Treaty on Audiovisual Performances (Beijing Treaty) 2012. Available at https://www.wipo.int/treaties/en/ip/beijing/.
30. CDPA, s.17; Designers Guild Ltd v Russell Williams (Textiles) Ltd (t/a Washington DC) [2002] 1 WLR 2416; Temple Island Collection Ltd v New English Teas Ltd [2012] EWPCC 1.
31. CDPA, s.12-s.15; CDPA, s.16(2); The Electronic Commerce (EC Directive) Regulations 2002 No 2013 available at https://www.legislation.gov.uk/uksi/2002/2013/contents/made.
32. CDPA, s.1–8, s.153–156.
33. CDPA, s.12-s.15 contrast with s.191 (Copyright, Designs, and Patent Act 1988, c 48 available at https://www.legislation.gov.uk/ukpga/1988/48/contents).

## References

Arnold R (2016) Performers' rights. London, England: Sweet & Maxwell.

Bliss L (2019) The protection from Harassment Act 1997: failures by the criminal justice system in a social media age. *The Journal of Criminal Law* 83(3): 217–228.

Blythe SM (2019) Freedom of speech and the DMCA: abuse of the notification and takedown process. *European Intellectual Property Review* 41(2): 70–88.

Bode L (2021) Deepfaking Keanu: Youtube deep fakes, platform visual effects, and the complexity of reception. *Convergence: The International Journal of Research into New Media Technologies* 27(4): 919–934.

Caldera E (2019) Reject the evidence of your eyes and ears: deepfakes and the law of virtual replicants. *Seton Hall Law Review* 50: 177–206.

Campbell J (2020) The origins and development of the right to privacy. In: Koltay V and Wragg P (eds). *Comparative Privacy and Defamation*. Cheltenham, UK: Edward Elgar, 9–23.

Carty H (2012) Passing off: frameworks of liability debated. *International Philosophical Quarterly* 2: 106–122.

Chan C, Ginosar S, Zhou T, et al. (2018). Everybody can dance now. *arXiv:1808.07371v1 [cs.GR] 22 August 2018*, pp. 1–9.

Chesney R and Citron D (2019a) Deep Fakes: a looming challenge for privacy, democracy, and national security. *California Law Review* 107(6): 1753–1820

Chesney R and Citron DK (2019b) 21st century-style truth decay: deep fakes and the challenge for privacy, free expression, and national security. *Maryland Law Review* 78(4): 882–891.

Coors C (2015) Opinion or defamation? Limits of free speech in online customer reviews in the digital era. *Comms. L* 20(3): 72–77.

Deazley R (2003) Introducing publicity rights–breach of confidence, the photograph and the commodifying the image. *Northern Ireland Legal Quarterly* 54(2): 99–117.

Deazley R (2017) Chapter 7: Copyright and Digital Cultural Heritage: Exceptions to Copyright. *The Copyright Cortex*. Available at: https://copyrightcortex.org/copyright-101/chapter-7

Delfino RA (2020) Pornographic deepfakes: the case for federal criminalization of revenge Porn's next tragic act. *Actual Problems of Economics and Law* 1: 150–214.

Deng K, Bansal A, and Ramanan D (2020) *Unsupervised Any-to-Many Audiovisual Synthesis via Exemplar Autoencoders. arXiv Preprint arXiv:2001.04463. 13 January 2020*. Available at: https://arxiv.org/abs/2001.04463

Edwards L and Harbinja E (2013) 'What happens to my Facebook profile when i die?' Legal issues around transmission of digital assets on death. In: *Maciel C and Pereirar) Digital Legacy Interaction. Human-Computer Interaction Series*. Cham: Spring. pp.115–144.

Ekaratne SC (2020) Manipulated images: a taxonomy. *European Intellectual Property Review* 42(6): 353.

European Commission (2021) Proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts. COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Farish K (2020a) Do deepfakes pose a golden opportunity? Considering whether english law should adopt California's publicity right in the age of the deepfake. *Journal of Intellectual Property Law & Practice* 15(1): 40–48.

Farish K (2020b) Deepfakes. *Practice Notes Lexis PSL*.

Fletcher J (2018) Deepfakes, artificial intelligence, and some kind of Dystopia: the new faces of online post-fact performance. *Theatre Journal* 70(4): 455–471.

Franks MA and Waldman AE (2019) Sex, lies and videotape: deep fakes and free speech delusions. *Maryland Law Review* 78(4): 892–898.

Garstka K and Polanski P (2019) Notice and search-down injunctions in online copyright enforcement: should they be embraced or forgotten? *European Intellectual Property Review* 41(3): 155–162.

Gibson J (2020) Where have you been? CGI film stars and reanimation horrors. *Queen Mary Journal of Intellectual Property* 10(1): 1–6

Gomery G (2007) Whose autonomy matters? Reconciling the competing claims of privacy and freedom of expression. *Legal Studies* 27(3): 404–429.

Greenberg D (2021) Communications offences. *Westlaw Edge UK*. 26 February 2021.

Griffiths J (2013) Dematerialisation, pragmatism and the European copyright revolution. *Oxford Journal of Legal Studies* 33: 767–790.

Harbinja E (2017) Post-mortem privacy 2.0: theory, law, and technology. *International Review of Law, Computers & Technology* 31(1): 26–42.

Helm RK and Nasu H (2021) Regulatory responses to 'fake news' and freedom of expression: normative and empirical evaluation. *Human Rights Law Review* 21: 302–328.

Ice J (2019) Defamatory political deepfakes and the first amendment. *Case Western Reserve Law Review* 70(2): 417–455.

Jacques S (2019) *The Parody Exception in Copyright Law*. Oxford, England: Oxford University Press.

James B (2020) Why you and the court should not accept audio or video evidence at face value: how deepfake can be used to manufacture very plausible evidence. *International Family Law* 23(2). pp. 43–45

Kietzmann J, Mills AJ, and Plangger K (2020) Deepfakes: perspectives on the future "reality" of advertising and branding. *International Journal of Advertising* 40(3). pp. 1–13.

Kirchengast T (2020) Deepfakes and image manipulation: criminalisation and control. *Information & Communications Technology Law* 29(3): 308–323.

Kugler MB and Pace CL (2021) Deepfake Privacy: Attitudes and Regulation. Northwestern University Law Review 116 Epub ahead of print. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3781968.

Kwok AOJ and Koh AGM (2020) Deepfake: a social construction of technology perspective. *Current Issues in Tourism* 24(3). pp.1–5.

Lees D (2021) Could Deepfake films make their way from YouTube novelty and artworld provocation into mainstream cinema? *Sight & Sound, Rushes Technology* 2021: 1.

McDonagh L (2021) *Performing Copyright: Law, Theater and Authorship*. Oxford, UK: Hart Publishing.

Meskys E, Liaudanskas A, Kalpokiene J, et al. (2020) Regulating deep fakes: legal and ethical considerations. *Journal of Intellectual Property Law & Practice* 15(1): 24–31.

Mirsky Y and Lee W (2021) The creation and detection of deepfakes: a survey. *ACM Computing Surveys, Prepub Ahead of Print. arXiv:2004.11138*. 10.1145/3425780. pp.1–41. Available at: https://arxiv.org/abs/2004.11138.

Montasari R, Peltola P, and Carpenter V (2016) Gauging the effectiveness of computer misuse act in dealing with cybercrimes. In: International conference on cyber-security and protection of digital services 2016, London, UK, 13–14 June 2016, 1–5. DOI 10.1109/CyberSecPODS.2016.7502346.

O'Connell A (2020) Image rights and image wrongs: image-based sexual abuse and online takedown. *Journal of Intellectual Property Law & Practice* 15(1): 55–65

O'Connell A and Bakina K (2020) Using IP rights to protect human rights: copyright for 'revenge porn' removal. *Legal Studies* 40(3): 442–457.

Oke EK (2020) Image rights and passing off: should reputation be enough for celebrities to succeed in English courts? *Journal of Intellectual Property Law & Practice* 15(1): 49–54.

Pavis M (2016a) Is there any-body on stage? A legal (mis)understanding of performances. *The Journal of World Intellectual Property* 19(3): 99–114.

Pavis M (2016b) *The Author-Performer Divide in Intellectual Property Law: A Comparative Analysis of Australia, France, the United Kingdom and the United States*. PhD Thesis, University of Exeter, UK.

Pavis M (2018) Runway models, runway performers? Unravelling the Ashby jurisprudence under UK law. *Journal of Intellectual Property Law & Practice* 13: 867–877.

Pavis M (2019) 'In fashion, one day you in, the next you are out': comparative perspectives on the exclusion of fashion models from performers' rights. *European Intellectual Property Review* 41(6): 347–358.

Pavis M (2020) Submission to the UK IPO: artificial intelligence and performers' rights. pp. 1–28. DOI: 10.5281/zenodo.4298854. Available at: https://zenodo.org/record/4298855#.YE_.

Pavis M (2021a) Regulating deepfakes using performers' rights. *Internet Newsletter for Lawyers* (January 2021). Available at https://www.infolaw.co.uk/newsletter/2021/01/regulating-deepfakes-using-performers-rights/

Pavis M (2021b) The protection of performances fixed in audiovisual recordings under UK Law and the Beijing – submission to the UK IPO. pp. 21–22 [in press]

Pechenik Gieseke A (2020) 'The new weapon of choice': law's current inability to properly address deepfake pornography. *Vanderbilt Law Review* 73(5): 1479–1516.

Perrot E and Mostert F (2020) Fake it till you make it: an examination of the US and English approaches to persona protection as applied to deepfakes on social media. *Journal of Intellectual Property Law & Practice* 15(1): 32–39.

Pihlajarinne T (2017) Should we bury the concept of reproduction – towards principle-based assessment in copyright law? *International Review of Intellectual Property and Competition Law* 48(8): 953–976

Rothman J (2018) *The Right of Publicity: Privacy Re-imagined for a Public World*. Cambridge, MA: Harvard University Press.

Rudkin T (2014) Things get serious: defining defamation. *Entertainment Law Review* 25(6): 201–204

Saied A (2020) Reid v price – Calculation of damages for breach of confidence, misuse of private information, breach of contract and compensation under the data protection Act 1998. *Entertainment Law Review* 31(5): 171–174.

Schwiddesssen S, Clark B, Defaux T, et al. (2018) Germany's network enforcement act – closing the net on fake news? *European Intellectual Property Review* 40(8): 539–546.

Silbey J and Hartzog W (2019) The upside of deep fakes. *Maryland Law Review* 78(4): 960–966.

Simone D (2019) *Copyright and Collective Authorship – Locating the Authors of Collaborative Work*. Cambridge, UK: Cambridge University Press.

Smith M (2020) *Malicious Falsehood*. Westlaw Edge UK.

Tan D (2017) *The Commercial Appropriation of Fame: A Cultural Analysis of the Right of Publicity and Passing off*. Cambridge University Press.

UK Intellectual Property Office (2020) Artificial Intelligence and intellectual property: a call for views (Published 7 September 2020). Available at: https://www.gov.uk/government/consultations/artificial-intelligence-and-intellectual-property-call-for-views (accessed 2 June 2021).

UK Intellectual Property office (2021), Beijing Treaty on Audiovisual performances: call for views (Published 23 April 2021). Available at: https://www.gov.uk/government/consultations/beijing-treaty-on-audiovisual-performances-call-for-views (accessed on 2 June 2021).

UK Law Commission (2018) Abusive and Office Online Communications: A Scoping Report. *Law Com No 381. HC 1682*. Available at: https://www.lawcom.gov.uk/abusive-and-offensive-online-communications/ (accessed on 16 March 2021)

Wadlow C (2016) *The Law of Passing-off: Unfair Competition by Misrepresentation*. UK: Sweet and Maxwell.

Waever R (2020) Defamation: a half-century of changes (more or lesss). In: Koltay V and Wragg P (eds). *Comparative Privacy and Defamation*. Cheltenham, England: Edward Elgar, 243–252.

Walsh K, Wallace A, Pavis M, et al. (2021) Intellectual property rights and access in crisis. *International Review of Intellectual Property and Competition Law* 52: 379–416

Westerlund M (2019) The emergence of Deepfake technology: a review. *Technology Innovation Management Review* 9(11): 39–52.

Whyte C (2020) Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of Cyber Policy* 5(2): 199–217.

Wragg P (2020) Separated by a common language: the anti-paternalism principle in US and English defamation and privacy law. In: Koltay V and Wragg P (eds). *Comparative Privacy and Defamation*. Cheltenham, England: Edward Elgar, 65–79.

Yamaoka-Enkerlin A (2020) Disrupting disinformation: Deepfakes and the Law. *New York University Journal of Legislation and Public* 22(3): 725–750.

Zakharov E, Shysheya A, Burkov E et al. (2019) Few-shot adversarial learning of realistic neural talking head models. In Proceedings of the IEEE/CVF international conference on computer vision 2019, IEEE Explore. pp. 9459–9468. Available at: https://openaccess.thecvf.com/content_ICCV_2019/papers/Zakharov_Few-Shot_Adversarial_Learning_of_Realistic_Neural_Talking_Head_Models_ICCV_2019_paper.pdf