Received: 28 October 2025 | Accepted: 9 March 2026

DOI: 10.1111/jwip.70020

ORIGINAL ARTICLE

THE JOURNAL OF WORLD INTELLECTUAL PROPERTY WILEY

Do deepfakes, digital replicas and human digital twins justify personality rights?

Dr. Hayleigh Bosher

Brunel University of London, London, UK

Correspondence
Dr. Hayleigh Bosher, Brunel University of London.
Email: Hayleigh.bosher@brunel.ac.uk

Abstract

Unauthorised deepfakes are deeply problematic, from the spreading of misinformation to non-consensual pornographic content. This paper asks whether deepfakes, digital replicas and human digital twins justify personality rights. To address this question, it examines the harms that deepfakes can cause through disinformation, demeaning content and displacing creative workers. It demonstrates that the current UK legal patchwork of passing off, intellectual property, defamation, and criminal laws do not adequately address these harms. Therefore, it proposes the introduction of personality rights into UK law, in the form of an automatic unwaivable personality right for 70 years after the death of the person, with appropriate exceptions to protect freedom of expression. Deepfakes are the hinges on which to open the door of personality rights in the UK, for protection against the harms of unauthorised digital replicas.

KEYWORDS

artificial intelligence, deepfakes, digital replicas, human digital twins, personality rights, synthetic media

1 | INTRODUCTION

Deepfakes are a type of synthetic media, such as images, videos, or audio, that are generated by artificial intelligence (AI) technology.[1] The origins of deepfake technology began with specific narrow uses such as in Hollywood movies.[2] Today, it spans multiple uses in a variety of industries, from medical intervention to translation. For example, artist Randy Travis was able to release new music for the first time since suffering a stroke using deepfake technology that cloned his own voice,[3] and a Malaria No More campaign used deepfake videos of celebrity David Beckham appealing to the public in nine different languages, enabling the charity to increase accessibility of their message to a wider audience.[4]

However, like any technology, it is capable of both utility and misuse. This is amplified by the development of social media, faster processors, high-performance graphics cards and smarter algorithms, instituting a major leap forward in the accessibility and capability of the technology.[5] It has become so sophisticated and readily available that no expertise is required to produce unauthorised replicas.[6] The result is skyrocketing numbers of deepfakes, increasing 550% from 2019.[7] By 2024 there were 2298 tools for AI face swap and lip sync, 10,206 tools for image generation, and 1018 tools for AI voice generation and voice cloning.[8]

It is unsurprising then that deepfakes are considered to be a 'critical threat to individuals and society.'[9] Alex Davis Jones MP described deepfakes as a 'threat to democracy' and Tom Tugendhat MP warned that they 'threaten our freedom.'[10] The UK Government has recognised 'the proliferation of these hyper-realistic images has grown at an alarming rate, causing devastating harm to victims, particularly women and girls who are the primary target.'[11] Hence, legislators around the world are considering and implementing deepfake regulation.

This paper asks whether deepfakes, digital replicas and human digital twins justify personality rights. To address this question, it first brings together the literature on the harms of deepfakes. Whilst there are currently papers that touch upon the general harms, or look specifically at one harm, this article fills a gap by drawing together the key harms, including developing of the harms identified by Ofcom.

It then provides an analysis of the UK legal landscape, to map the current legislative and common law remedies that may serve a victim of unauthorised deepfakes. Whilst there is literature that touches on some of these legal areas, or specifically focuses on one area, this paper contributes to the discourse by providing a holistic overview across all legal possibilities. The need for this research was identified by civil servants, academics and policy experts at UK Government roundtables on artificial intelligence.

Recognising the harms of deepfakes together with the merging of personhood and technology, the paper concludes that the patchwork of UK law is inadequate in addressing those harms. Therefore, the paper argues that these circumstances do justify the expansion of protection, and proposes the introduction of personality rights as a solution. It argues for an unwaivable, automatic personality right, embedded in the current copyright regime, aligned with the term of copyright protection and appropriate exceptions.

2 | THE HARMS OF UNAUTHORISED DEEPFAKES

The term *deepfake* emerged around 2017, bringing together the concepts of *AI deep-learning* and *fake*, since the content is not real; essentially 'shorthand for the full range of hyper-realistic digital falsification of images, video, and audio.'[12] The technology enables the manipulation of image to swap a face, body or voice, for another. It is designed to continuously develop its performance, so the algorithm learns and improves, making the outputs increasingly realistic.[13] Typically, the term deepfake is used in the context of wrongdoing, although not exclusively, while 'digital replica' has been adopted by certain stakeholders as more neutral language. Both refer to the same technology, so this paper uses the terms interchangeably. A digital twin is a digital version of something, or someone, that exists in real life and could also be encapsulated as a digital replica. Therefore, human digital twin (HDT) is used only when referring to the specific issues arising from that technology.

Traffic to websites that host deepfakes is growing, resulting in profitable businesses that generate income through advertising and subscription models. Users can pay for digital replicas to be produced, for example, one individual made over $74,000 generating unauthorised deepfakes.[14] As such, the creation and dissemination of deepfakes has 'moved from a custom service available on niche internet forums to an automated and scaled online business.'[15]

A broad range of actual and potential harms arising from unauthorised deepfakes have materialised. The following section highlights three major categories of concerns: disinformation, demeaning content, and displacing creative workers. These categories echo the harms outlined by Ofcom which are those that defraud and demean.[16] However, this analysis adds the harm of displacement, on account of the creative workers whose livelihoods are under threat by AI.

2.1 | Disinformation and fraud

Deepfakes create significant cybersecurity challenges such as identity theft, scams, and increasing misinformation campaigns and reputation attacks. For example, Know Your Customer (KYC) fraud involves using deepfakes to defeat facial recognition detection systems to bypass security measures, enabling unauthorised access to financial services and sensitive personal accounts.[17]

It is becoming increasingly difficult to distinguish between real and fake content,[18] leading to people being misled. As the United States (US) Copyright Office observed, 'an era of sophisticated digital replicas has arrived.'[19] Deepfakes videos have advanced to even exhibit heart rates which render them indistinguishable from real people.[20] This is concerning because people tend to believe what they see.[21] Ofcom found that 61% of social media users who said they were confident in judging whether online content was true or false were unable to do so.[22] Anyone can be misled, including the chief executive of a UK-based energy company who transferred €220,000 because of a deepfake scam.[23] Other uses of fraudulent deepfakes include digital evidence used in court,[24] which erodes trust in video evidence, reducing its probative value.[25] Perpetrators are also utilising deepfakes to commit dating scams, for example, the National Fraud Intelligence Bureau received 8036 reports of romance fraud, amounting to over £92 m lost by victims in 2022.[26]

Another concern is that deepfakes enable fraudulent impersonation scams by appropriating the identity of individuals, such as an advertisement for investment featuring Martin Lewis on social media that was found to be a deepfake.[27] The existence of digital replicas in our information ecosystem can have a corrosive effect on our reality and become an agent of chaos.[28] Such as the automated telephone call which delivered a recorded message using fake audio of US President Joe Biden made to New Hampshire voters, urging them to stay home during the election.[29] In the UK, a counter-terror investigation was launched after a deepfake of London Mayor Sadiq Khan backing a pro-Palestine protest on Armistice Day was released. Khan reflected, 'we almost had serious disorder' and that this type of deepfake could have a worrying broader impact such as a close election or referendum, or where there is community unrest.[30]

The UK Science, Innovation and Technology Select Committee (SITC) reported that AI is 'lowering the barrier of entry into cybercrime, making it easier for cyber attackers to successfully target victims and widening the availability of voice cloning, deepfakes and social engineering bots.'[31] Thus, deepfakes can cause harm in the form of fraudulent use and the spread of disinformation.

2.2 | Demeaning content

Another category of harm is caused by one of the most common and disturbing uses of deepfakes; to create explicit images and videos without consent.[32] As early as 2019, a study demonstrated that 96% of all deepfakes online were pornographic in nature.[33] At that time the technology was less accessible, whereas now, anyone can easily generate pornographic content using apps that 'undress' a person or replace their face with that of sex worker without consent. By 2023, 98% of all unauthorised deepfakes online were pornographic,[34] in fact, that same year more deepfake abuse videos were posted than every other year combined.[35]

These non-consensual deepfakes disproportionately impact women and girls, with 99% targeting women[36] and many of the applications *only* work on women as the AI is only trained on female bodies.[37] They are used to humiliate, undermine and exploit individuals.[38] High-profile women, particularly those who are known for being vocal feminists, have been targeted[39] with pornographic deepfakes, with some including violence against the women. For example, a non-consensual deepfake of Taylor Swift, that was both sexual and violent in nature, was viewed by 47 million people within 24 h,[40] and there are over 1000 videos of Emma Watson on the leading deepfake porn website.[41]

Still, the most targeted group is non-celebrity women.[42] The Police Chief's Council identified online and tech-enabled violence against women and girls as a key high-harm threat, noting that there has been a 258% increase in survivors supported between 2018 and 2022. They observed that the emergence of generative AI provides another layer of complexity to this evolving threat.[43] Baroness Owen described deepfake abuse as a 'new frontier of violence against women.'[44]

The impact of this abuse can be a life-shattering, violating experience for survivors. The perpetrator is often unknown, creating fears about who they can trust and who has seen the content. Survivors have reported suffering from anxiety, Post Traumatic Stress Disorder, suicidal ideation, feeling that their bodily autonomy has been compromised,[45] and described the harm as pervasive across their social, economic, digital, sexual and political lives, in a continuous way.[46] Laura Bates recounted the layers of emotional and physical responses that she, and her interviewees, experienced on seeing themselves in deepfake pornography, from shock, panic, anxiety and illness, to 'the realisation that there may come a point in time when this video…this form of violence and control…might outlive you.'[47] Women have taken their own life as a result of this abuse.[48]

Telegram is an example of an application that generates deepfake explicit images. Seventy percentage of Telegram users were found to target women and, in July 2020, at least 104,852 explicit deepfakes had been shared in a 'image collections' channel available on the app.[49]

While it is not possible to know the full extent of deepfakes depicting children, research by My Image My Choice suggested there is a 'plethora of deepfakes dedicated to underage women and teens.'[50] Ofcom has estimated 17% of sexual deepfakes depict individuals under the age of 18.[51] The Children's Commissioner and the Internet Watch Foundation have both called for a total ban on apps that allow nudification, where images of real people are manipulated by AI to appear naked, condemning that such apps 'go unchecked with extreme real-world consequences' especially for children.[52] During a House of Lords debate, Lord Tim Clement-Jones asked the Online Safety Minister if the Government will act to ban these tools. The Minister responded that 'creating or distributing child sexual abuse images, is already illegal regardless of whether it depicts a real child or not.'[53] However, these laws alone are clearly inadequate deterrents for such behaviour since the number of deepfakes are growing exponentially. Combine the readily available deepfake pornography technology with the speed of developing AI and wearables, such as Meta AI glasses which can capture images and use AI to interact with the content,[54] and the imagination does not have to work very hard to envisage a near-future where these technologies and harms escalate beyond control.

It is already established that pornography can perpetuate harmful stereotypes across genders and ethnicities.[55] A government-commissioned review concluded that there is substantial evidence to show a clear relationship between pornography and harmful attitudes and behaviours towards women and girls. The study reported that pornography use has been associated with an increased likelihood of committing both verbal and physical acts of sexual aggression.[56] This is elevated by non-consensual deepfake pornography, which are malign expressions of misogyny and part of a continuum that can lead to real-world violence.[57] The correlation between image-based abuse and escalating physical violence is widely accepted.[58] The Police have acknowledged the potential causal relationship between precursory and higher-harm offending.[59] The Angiolini Report, investigating how an off-duty police officer was able to abduct, rape and murder Sarah Everard, found that the perpetrator had a history of alleged sexual offending dating back 20 years, including sharing unsolicited intimate photographs. The report noted that masturbatory fantasy and rehearsal is commonplace prior to serious sexual offending. It noted the perpetrator's willingness to show friends violent and extreme pornography from 17 years before, and concluded that sexual deviants have a varied diet of perverted sexual interests that form part of a trajectory of escalating risk towards physical sexual violence.[60] Therefore, an additional concern is that the impact of non-consensual deepfake pornography will lead to increased contact-violence against women and girls. As Bates explains: 'If we do not take action now to stem the tide of deepfake image abuse, in the coming years we will see more and more cases of offences like stalking and murder that involve some element of manipulated sexual images.'[61]

Jacobsen and Simpson argue that non-consensual pornographic deepfake videos are less about if the videos pass as 'real' and more about reinforcing a patriarchal view of women. Deepfakes should be understood as forming part of a long genealogy of male-dominated ways of seeing, where women are docile and passive carriers of male desires.[62] Thus, it is irrelevant that the content is not 'real', the production and consumption of unauthorised deepfakes reinforce women's subjugated position in patriarchal society. Non-consensual deepfake pornography perpetuates misogynistic and patriarchal norms that result in individual and societal harms.

2.3 | Displacing creative workers

The third category of harm is using deepfakes to displace the work of performers and artists. In the creative industries, there are concerns of performers having their voice and image replicated without their permission, resulting in work lost to AI substitutes. Deepfake songs have been generated using the voice of artists, such as a song mimicking Drake and The Weeknd, without their knowledge or permission.[63] Likewise, deepfake samples have been used within songs, such as generating the voice of deceased rapper Tupac Shakur.[64]

Equity, the performing arts and entertainment trade union, have reported that 94% of performers think the Government should regulate deepfakes. Their survey revealed that 65% of performers and 93% of audio artists thought the development of AI poses a threat to their employment opportunities.[65] Projects that used digital replica extras instead of background actors already exist,[66] voice actors have been replaced with AI replicas in film[67] and game.[68] Celebrities have had their voice cloned, but as Lees commented, since the law is not up to date 'there's very little that David Attenborough can do.'[69] Therefore, the third category of harm caused by unauthorised deepfakes is displacing creative workers.

The above sections have set out three key categories of harm currently caused by unauthorised deepfakes. The following section highlights issues relating to HDTs.

2.4 | Human digital twins (HDTs)

The concept of the digital twin has its origins in the 1970s NASA Apollo program, where the idea of constructing identical space vehicles on Earth to predict the behaviour of those in space was first explored.[70] It then developed to become a digital modelling tool, for example, Amazon generated one to improve the efficiency of its factory floor. Amazon now provide a digital twin maker for developers to generate digital twins of real-world systems such as buildings, industrial equipment and production lines with the aim of optimising operations and improving performance.[71]

More recently the *human* digital twin has emerged, referring to the replica of a physical-world human in digital form, defined as a model or database which records current and historical human data.[72] Measurable attributes include physiological perceptual performance, cognitive performance, personality characteristics, emotional state, ethical stance, and behaviour.[73] In the work environment the HDT is able to simulate the behaviour, actions, and interactions of an employee by capturing data from tracking how the employee completes tasks, interacts with others, and meets productivity goals, analysing patterns in decision-making, stress levels, time management, collaboration, and creativity. Some models monitor physical well-being through wearable technology such as a smart watch and cognitive performance through task tracking and AI analytics. The technology is already being utilised across sectors from medicine,[74] to fitness[75] and recruitment.[76] These models utilise physical parameters, emotional status, and cognitive trends of a person to create the HDT, evolving to encompass autonomous, context-aware, and adaptive AI models.[77]

The aim of the HDT employee is to create a continuously updated model of the employee. HDT claims to have various purposes, from personalised skill development to optimising team dynamics, as well as interacting with the HDT when the employee is unavailable. Eightfold AI Digital Twin technology, for example, advertises that it can capture 'every employee's wisdom, knowledge, skills, and experiences. By seamlessly integrating across enterprise systems, email, messaging platforms including Teams, Slack, CRMs, project management tools, and code repositories' to 'capture the essence of each individual's work contributions—the decisions they've made, the networks they've nurtured, and the expertise they've built.' Eightfold suggest that their digital twin technology allows organisations to improve productivity and gives employers access to 'deep, continuous understanding of their people—not just as roles or titles, but as engines of insight, creativity, and value.'[78]

Since research and development of HDTs is in early stages, there is a distinct lack of comprehensive analysis of universal frameworks and applications,[79] with little-to-no consideration of the legal parameters. HDTs raise concerns relating to consent, privacy, control and ownership of the digital assets. In the context of employment, where there is a power disparity between employee and employer, there is no law that specifically deals with the issues of HDTs, and the application of existing law is uncertain. Employers may believe that they can lawfully collect, retain and use their employee's data and that the employee has no legal redress to stop this or to determine what software tools the employer utilises. However, this assumes that the copyright rules for work created in the course of employment would extend to all manner of data inputs.[80]

For the employee, pushing back on the employer's adoption of HDTs could result in loss of employment. Employees need protecting. Robust governance and policies are needed to oversee the ethical control and management of these digital assets.[81]

HDT technology is in its infancy; as it develops it will become accessible not just to employers but to everyone, in the same way that deepfakes started in Hollywood. As a result, the concerns will be magnified, incrementally building on the harms relating to deepfakes. 'Neurohacking' will become a risk, where hackers can access and manipulate data affecting the human or HDT, resulting in the redistribution of agency from the user or host to the hacker. This poses a threat to the protection of personhood through unauthorised access to the human body and/or its digital twin. The merging of personhood and technology challenges legal definitions and applications, this in turn extends the physical limits of the human body and arguably expands the scope of the protection of personality and property relations.[82]

The speed at which this technology is multiplying will correlate with increasing such harms, without any safeguards in place it will exacerbate the inequalities of society. This section has examined the harms caused by deepfakes, the next section evaluates whether the current law adequately addresses these harms. Since the findings reveal a patchwork of ineffective regulation, this leads to the justification of exploring personality rights as a tool for addressing the harms of deepfakes.

3 | THE CURRENT UK LAW APPLICABLE TO DEEPFAKES

This section examines the applicability of passing off, trade mark, privacy, defamation, criminal offences, copyright, performers rights and technical solutions to deepfakes.

3.1 | Passing off

Passing off is a common law tort, established across the jurisdictions of the UK, that can allow a person to protect their reputation. The purpose of passing off is to prevent a trader from misleading customers by representing their goods or services as emanating from another. Where a claimant can demonstrate goodwill, misrepresentation, and damage to goodwill, they are able to prevent the unauthorised use of their name or images.[83] However, it is considered particularly difficult to achieve this and only applies in narrow circumstances.[84]

In the case of *Fenty* v *Arcadia*,[85] singer-songwriter Rhianna sued retail company Topshop after it sold a t-shirt featuring Rihanna's face. The court specifically stated that image rights do not exist under the law of England and Wales. However, Rihanna was able to succeed in her claim because she could demonstrate goodwill, misrepresentation, and damage to goodwill, being a celebrity that trades off her image, leading people to think that the shirt was official merchandise. This demonstrates that celebrities can rely on passing off in certain circumstances, but it may not apply to deepfakes. Firstly, the claim must prove that the consumers were deceived into thinking that the use was approved, which Perot argues is unlikely given the nature of digital replication.[86] Context was important in the Fenty case, as Justice Birss stated: 'Topshop is not a market stall. It is a leading high street fashion retailer and purchasers would not be surprised to find goods on sale in Topshop which have been endorsed or approved by celebrities.'[87] This was the reasoning in the decision not to grant an interlocutory injunction in the earlier case of *Lyngstad* v *Anabas*,[88] where music group, ABBA, were unable to prevent the defendants from using their pictures on merchandise because, the court held, there was no confusion.[89]

Passing off claims can be made in circumstances of false endorsement. The first successful UK action of this type was *Irvine* v *Talksport*.[90] Talk Radio manipulated an image of Eddie Irvine holding a phone, replacing the phone with a branded radio. The claim was upheld as passing off in the context of false endorsement. Much like the Rihanna case, this demonstrates that passing off may be a possible form of action for celebrities who trade from their image if a deepfake was used to endorse a product without permission.

However, this action falls short of protecting performers in the context of film, television, or narration. Likewise, this action has no relevance to individuals who do not trade off their image. Therefore, unhelpful to those who are victim to non-consensual deepfakes without goodwill, leaving many of the harms unaddressed.

Moreover, because passing off is limited to protection against misrepresentation, it will not protect against deepfakes where the relevant public is aware that a person is being imitated. As in the case of the television show 'Deep Fake Neighbour Wars,' created using performers who are face-swapped for well-known celebrities.[91] Since many digital replicas are found on websites specifically marketed for hosting deepfakes, the initial audience, at least in these circumstances, would understand that the content is not real, therefore passing off would not apply.

3.2 | Trade marks

Trade Marks are similar to passing off in that they are consumer-focused and protect a commercial interest in trade. Trade marks are registered monopolies of a brand name, logo or slogan,[92] and can, in certain circumstances, be extended to a movement, such as a victory pose by an athlete, for example when Mo Farah registered his signature 'Mobot' sign.[93] Names themselves are not protectable as property rights, but can be registered as trade marks when they are used in the course of trade,[94] for example, singer Sir Cliff Richard has several registered trade marks including his name and signature.[95] In rarer occasions, applicants have been successful in registering a face, for example Dutch models Roos Abels and Marlijn Hoek were able to register their portraits for services of modelling.[96]

For trade mark protection to be utilised in the context of deepfakes, the person would need to have successfully filed trade marks for their name or face, which requires that they are trading using that sign as a marker to distinguish goods or services. Therefore, this remedy would be extremely limited and would not meet the broad range of harms caused by deepfakes.

3.3 | Privacy rights, data protection and breach of confidence

Privacy rights are human rights to prevent interference with a person's life, stipulating that personal information, including photographs, should not be shared publicly without permission.[97] Other personal information, such as home address, and sensitive personal data, such as sexual orientation, is protected under the Data Protection Act 2018. Breach of confidence protects information that has a 'quality of confidence about it' that was imparted in circumstances where there was an obligation of confidence, used without permission.[98]

The difficulty with privacy law as a remedy against deepfakes is that it only applies where there is a reasonable expectation of privacy.[99] The law determines there is not usually a reasonable expectation of privacy in a public place.[100] If a video or photo was obtained to create the deepfake through hacking or stealing, privacy rights could be engaged, but for the most part, this is unlikely to be the case. Likewise, for breach of confidence, the information must have been private and used without consent.[101] This would only be a possible remedy where the content was shared under those circumstances.

HDTs are built on a combination of data that would likely include both personal and sensitive personal data. In the context of employment, this may give some leverage to an employee to request the removal of their personal data from the system. However, there are two main contentions. Firstly, due to the power imbalance between the employer and employee, the employee may not feel able to make such a request without threatening their employment. Secondly, only some data will be clearly within the remit of the Data Protection Act 2018. Biometric data, for instance, seems likely to fall within the scope of medical data and therefore sensitive personal data for the purposes of the Act.[102] Where it does apply, a data subject has the right to rectification, erasure or restriction of processing their data.[103] However, the tools also ingest information such as communications made by the employee, including emails and phone calls, as well as other measures of productivity, these may fall under the property rights of the employer and in fact not be under the control of the employee.

Overall, privacy, data protection and breach of confidence are unlikely to be a useful remedy for most unauthorised deepfakes. Although other jurisdictions, such as France,[104] allow for private individuals to have a general right to control the dissemination of their image, the law of England and Wales does not provide this. Although Deazley argues that an action in confidence to prevent the publication of images taken without consent, in public, in a covert manner, is conceivable. He separates these rights from property rights, whereby their intention is to prevent harm, stating that confidence 'does not and should not serve any proprietary interests.'[105] The harms he mentions—embarrassment, self-consciousness or humiliation—relate closely to the demeaning harms of deepfakes. However, given the scope of the harms, and the context of the fast-evolving technology, perhaps it is time to consider a proprietary interest in one's image.

3.4 | Defamation

In England and Wales, the Defamation Act 2013 could protect a person if the deepfake is used in a defamatory way. In particular, Libel is a wrongful act that concerns the publication of material in writing or some other permanent form.[106] The test for what is defamatory requires that the content causes, or is likely to cause, serious harm to the victim's reputation and only applies if the content is untrue.[107] Although Scotland has different legislation, the test for serious harm is the same.[108] Serious harm is a relatively high threshold that must be demonstrated as fact, be more than merely substantial, is distinguished from hurt feelings and cannot be established solely by reference to the inherent tendency of words to cause harm to reputation.[109]

AI-generated content may be defamatory.[110] If the digital replica shows a person doing something that they did not do, which typically encapsulates the purpose of deepfakes, then it could apply. The first defamation case against AI was threatened by an Australian Mayor, against a Chatbot that incorrectly named him as a guilty party in a foreign bribery scandal, but the claim was later abandoned.[111] There has yet to be any formal legal action in these circumstances. Given the number of non-consensual deepfakes this indicates that a defamation claim may not be viable. This may be due to the test for demonstrating reputational harm, the particularly high costs of defamation claims, or the difficulties arising from the fact that most deepfakes are posted anonymously. Shaw and Jackson argue that in these circumstances, a Norwich Pharmacal Order[112] could be made, requesting a website operator to disclose the identity of an anonymous publisher.[113] The website operators themselves can avoid liability through showing that it was not them who posted the statement on the website.[114]

Defamation law focuses on the act of publication, rather than creation. Without any legal precedent the question of liability remains unanswered. If a user downloads an app that can create a pornographic deepfake, and allows other users to view and share it, are those users liable? Or the app developers? In the case of *Bunt* v *Tilley*, a defamatory statement was published on a website, the court held that to be liable for a defamatory publication a defendant must be knowingly involved in the process of publication. The website played a passive instrumental role in the process and so could not be deemed a publisher.[115] Lavy and Munro argue that since a developer is defining the input and the output parameters it should no longer be regarded as simply facilitating, suggesting that it should qualify as publication. Although even they recognise that the automation of AI will pose a challenge.[116] This has yet to be tested in court leaving the application of defamation law to deepfakes to be uncertain at best and irrelevant at worst.

3.5 | Criminal offences relating to explicit content

One in every three deepfake tools allow users to create deepfake pornography, with 99% of the individuals targeted in these tools being women.[117] A 2020 study revealed that there are divergent, multifaceted and overlapping motivations for engaging in image-based sexual abuse, including revenge, sexual gratification, social status or financial gain, with power and control presenting as overarching themes. The study emphasised the importance of recognising the gendered nature of these behaviours and the connections to masculine entitlement and privilege. Moreover, it argued that the non-consensual taking or sharing of explicit images has become a normalised practice and advocated for criminal laws, as well as other interventions, to address image-based sexual abuse.[118] Deepfake pornography is a new form of abuse that is not just about sexualising women, but serves as an instrument of power, control and subjugating women. This is acutely apparent in the deepfakes that include violence and mocking.

In the circumstances of explicit deepfakes, some areas of legislation may be applicable. Since 2015, the law has prohibited the sharing of real private, sexual photos or videos of another person without their consent.[119] In 2021 this was updated to include threatening to disclose intimate sexual images.[120] Upskirting—taking a picture under a person's clothing without their knowledge—was criminalised in 2019.[121] And, in 2023 an offence for sharing, or threatening to share, 'intimate images'[122] including deepfakes was legislated.[123] A person convicted of this offence can be imprisoned for up to 2 years.[124] Given the rising number of pornographic deepfakes online this does not appear to be a strong enough deterrent.[125] By comparison, a person convicted of online copyright infringement can serve up to 10 years' imprisonment.[126]

The definition of an intimate image, for the purposes of this offence, includes showing genitals, people engaged in a sexual act or intimate areas of someone's body, up-skirting, down-blousing and breastfeeding.[127] This has been criticised as a White, Western definition of intimacy that leaves some women unprotected.[128] The amendments do not address deepfakes that constitute other demeaning behaviours, such as the removal of a headscarf for a woman who chooses to wear one. A broader or subjective definition may be more appropriate.

A further weakness of this approach is that it only criminalised the *sharing* of intimate deepfakes, not the *creation* of them. However, in January 2025, the Ministry of Justice announced that the Government intended to crackdown on explicit deepfake predators by making the *creation* of explicit deepfakes a criminal offence, with perpetrators also facing up to 2 years in prison.[129] As part of this development, the upskirting offence will be repealed, along with the offence for recording of a person doing a private act, to be replaced with three new offences that cover a broader range of behaviour.[130] The amendment to the Data (Use and Access) Act 2025 came into force on 6 February 2026.

Criminalising the creation of intimate deepfakes could encourage cultural change and impose stronger obligations on hosting platforms, as Clare McGlynn explained: 'If creation of pornographic deepfakes was unlawful, it would be difficult for payment providers to continue to prop up the deepfake ecosystem, difficult for Google to continue returning deepfake porn sites at the top of searches and difficult for social media companies such as X (formerly Twitter) or the app stores to continue to advertise nudify apps.'[131]

Nevertheless, the Government stopped short of criminalising *possession* of non-consensual intimate images or mandating internet service providers to act against content hosted overseas. Baroness Bertin criticised that 'the current offences do not go far enough.'[132] Andrea Simon, Director of the End Violence Against Women Coalition, called this a 'missed opportunity to deliver justice for survivors and prevent future harm.'[133] It means that a person is not committing any offence by requesting the creation of, or keeping, a deepfake for themselves. It is therefore argued that possession of an unauthorised deepfake should be included in the criminal offence, in line with possession with other comparable offences such as relating to child sexual images.[134] There are no legitimate reasons to legalise the possession of explicit unauthorised deepfakes.

A further limitation is that, whilst the current law prohibits non-consensual distribution of private, sexual images, it does not include altered or AI-generated images and fails to encapsulate deepfake cyberflashing.[135] These are significant failings of the law that require urgent revision.[136]

These legal changes were originally proposed by the previous Conservative Government in the Criminal Justice Bill, but it did not make it through before the dissolution of Parliament.[137] The current Labour Government picked up the issue and announced[138] that the amendments would form part of the Crime and Policing Bill.[139] Further delays ensued and the proposals were moved to the Data (Use and Access) Bill, with the aim 'to ensure the new law is on the statute book as quickly as possible.'[140] However, the Data Bill became controversial, going back and forth from the Commons to the Lords over issues relating to AI transparency. During these delays the Women and Equalities Committee emphasised the need for the Government to take a consent-based approach to implementing this law and 'not require the determination of any motivation on the part of the perpetrator.'[141] Following its Inquiry into Non-Consensual Intimate Image Abuse, the Committee made it clear that 'there is no legitimate reason whatsoever for the use or existence of nudification apps.' Their report recommended that the use of such applications be a criminal offence, that Ofcom should investigate sites that offer this functionality and that the Government should ensure search engines and platforms that promote or facilitate the distribution of such apps are held accountable.[142]

In its response, the Government agreed that the new law would be a 'consent-based' offence. However, it rejected the need for stronger regulation of platforms and search engines, claiming that there are already a range of regulatory requirements that apply. It also rejected the recommendation to make possession of non-consensual intimate images an offence, saying that it would be too difficult to establish whether consent had been obtained in these circumstances.[143]

Disappointed with this, the Women and Equalities Committee urged the Government to bring forward the legislative proposals, saying that if it fails to do so, the Committee will put forward its own, in the form of amendments to proposed legislation.[144] Nevertheless, the Data (Use and Access) Act received Royal Assent on 19 June 2025 without such amendments.

In practice, criminal laws such as these depend on the Crown Prosecution Service (CPS) to pursue charges against the perpetrator. This means that individuals must report the incident to the police and rely on them to take it forward. Despite clear evidence of the direct and wider harms of non-consensual intimate deepfakes, Bliss points out that failure by the police and CPS to link online abusive content to the behaviours of stalking and harassment has resulted in devastating consequences.[145] Not to mention that the criminal justice system is struggling with timeliness; both Magistrates' and Crown Courts have huge backlogs which continue to increase.[146] When only 2.6% of rape cases result in a conviction/summons, it leaves doubt as to the effectiveness of the new criminal offences in protecting victims.[147] Regulating unauthorised deepfakes more strongly is required to send a clear message that this behaviour is unacceptable, but without effective enforcement, the offences are meaningless to victims.

The Government has asserted that it will halve violence against women and girls within a decade,[148] but the current law does not adequately address the harms of demeaning content that disproportionately affects women and girls. While it is a criminal offence for a person to create, share, or threaten to share, explicit deepfakes, the law falls short of criminalising possession of a deepfake, deepfake cyberflashing, or deepfakes of a demeaning nature other than explicit.

3.6 | Fraud and other criminal offences

The Protection From Harassment Act 1997 protects victims from stalking behaviour. Harassment is 'repeated attempts to impose unwanted communications and contact upon a victim in a manner that could be expected to cause distress or fear in any reasonable person.'[149] Under the Act, stalking includes publishing any statement or other material relating, or purporting to relate to, a person, or purporting to originate from a person,[150] amongst other behaviours.[151] Stalking and harassment accounts for 85% of all online and tech-enabled offences.[152] Since the legislation includes publishing material relating to, or purporting to relate to, or originating from a person, the offences of stalking could arguably apply to deepfakes, in certain circumstances. Likewise, if the perpetrator uses a deepfake in repeated unwanted contact, the offence of harassment may apply.

Other possibly relevant criminal offences relate to communications offences, such as false communication, where a person conveys information that they know to be false, which is intended to cause non-trivial psychological or physical harm to a likely audience.[153] This offence may be relevant where a deepfake is used to defraud or misinform with false information.

The Fraud Act 2006 legislates a criminal offence to dishonestly make a false representation, where the person intends to make a gain for themself or another and to cause loss or risk of loss.[154] While existing law relating to fraud remains unchanged, the type and sophistication of fraud has evolved with the development of deepfake technology.[155] A 2024 study found that fraud attempts using deepfakes have increased by 2137% over the last 3 years.[156] Yet, there have been no claims of fraudulent use of deepfakes in the courts of England and Wales. The only mention of AI fraud is in the case of *COPA* v *Wright* [2024], where the defendant utilised large language model, Chat GPT, to assist in fraud by generating fake content to support a false claim.[157] That said, deepfakes have reportedly been found in the courtroom in the form of fraudulent evidence,[158] which has adverse effects on the probative value of video evidence in court.[159]

The use of deepfakes to spread misinformation can have wider impacts if used to threaten democracy or national security. The National Cyber Security Centre has acknowledged that AI will make the spread of disinformation easier and deepfake campaigns will likely become more advanced.[160] The SITC recommended that the Government safeguard the democratic process by ensuring that platforms remove deepfake content and where platforms are slow in doing so, or facilitate the spread of deepfake misinformation, they 'must take stringent enforcement action—including holding senior leadership personally liable and imposing financial sanctions.'[161] Furthermore, the Committee called for improved public awareness on the growing prevalence of AI-assisted misinformation.[162]

However, the Government was unmoved, declaring that it already has robust systems in place to monitor and mitigate risks relating to AI and disinformation from hostile state actors, including techniques to counter disinformation and address sophisticated cyber threats.[163] It seems unlikely then that any reform to address increasing risks and harms relating to fraud and disinformation caused by deepfakes will be introduced in the near future.

3.7 | Copyright

Copyright is a legal right that prevents the copying of, amongst other things, photos and videos.[164] Although the primary purpose of copyright is to promote the creation and dissemination of creative works,[165] it has been utilised in actions to address a different harm, such as breach of privacy,[166] since copyright can be more straightforward to enforce. Therefore, a victim of non-consensual deepfake abuse could bring an action for copyright infringement, which provides remedies such as destruction of infringing copies and damages.[167] However, in order to bring an infringement claim, the victim must be the copyright holder.[168] The rightsholder is usually the person who took the photo or made the video.[169] This means that a copyright claim is only viable where the images or videos used in the face-swapping of the deepfake were taken by the victim. Moreover, enforcing this would be a challenge since there are currently no requirements for transparency in the use of copyright protected materials in the training or processing of AI.[170]

The second challenge is overcoming the test for infringement. Primary copyright infringement occurs when the whole, or a substantial part, of a copyright-protected work is copied without permission,[171] or the benefit of a copyright exception.[172] AI-generated deepfakes engage with copyright at two key stages; first the content input to train and process the AI tool, and second, the similarity between the copyright protected work and the AI-generated output.

On the first point, the question of whether the use of copyright protected material to train AI tools amounts to infringement is contentious. Whilst some academics and lawyers argue that the law is clear and permission would be required, AI technology developers argue that permission does not, or should not, be required. The issue is currently being tested in the case of *Getty Images* v *Stability AI*,[173] and is under Government consultation.[174] This leaves victims of non-consensual deepfakes with uncertainty in the interim, and no remedy if the Government sides with the view of the AI firms.

In relation to whether the AI-generated output constitutes primary copyright infringement, this requires that the output has taken a substantial part of the protected work.[175] It seems probable that, under the circumstances where the deepfake is intended to mimic the person from the original image, there would be a substantial similarity between the two. However, it is not without obstacles. The test for substantial part relates to the quality, and not the quantity,[176] of the parts taken. In this context, quality refers to the reason the work is protected by copyright; its originality.[177] It follows, then, that a claim for copyright infringement can be rebutted where the defendant can demonstrate that the work copied is unoriginal and consequently unprotectable.[178] In these circumstances, even where there was copying, it would not amount to copyright infringement.

Secondary copyright infringement may apply to the providers of the applications that generate deepfakes, since this includes providing means for making infringing copies.[179] Likewise, criminal copyright infringement may be relevant since it is an offence to make for sale or hire an infringing copy of a copyright work.[180] It is also a criminal offence to specifically design, or adapt, something that makes copies of a copyright work, where the designer knows, or has reason to believe, that it would be used to do so.[181] On the question of 'reason to believe' the Magistrate's Court has held that broad knowledge of the items complained of and the nature of the infringement is sufficient.[182] Therefore, developers, providers and hosts of deepfakes may be in breach of primary, secondary or criminal copyright infringement. That being so, a rightsholder would be able to choose their course of action from any forum available, including concurrent proceedings in the civil and criminal courts.[183] However, as mentioned, currently the application of copyright law to deepfakes, and AI more generally, is uncertain and under threat.

Where there is infringement, the question of who would be liable remains unclear. Liability may fall on the user that requested the AI to generate the deepfake, or on the developers and providers of the applications under primary or secondary infringement.[184] In the case of *Getty Images* v *Stability AI*, the rightsholders argued that liability falls with the technology developers—Stability AI—whereas, Stability AI argued that it should be on the individual users.[185] The question of primary liability was dropped at trial and secondary infringement was not found, although the Judge did state that if her finding was wrong Stability AI would be liable for secondary copyright infringement.[186] Therefore, currently there is no certainty that a copyright infringement claim would succeed, or indeed, who would be liable.

3.8 | Performer's rights

Performer's rights enable a performer to prevent someone recording a live performance without permission and stop unauthorised copies of their performance being shared.[187] This right is limited by the definition of what constitutes a performance. It only applies if the performer is acting, singing, dancing or performing a literary, dramatic or musical work.[188] It does not have to be a paid performance, but it is not clear exactly what does or does not qualify as a performance; magicians, clowns, jugglers, impersonations, interviews and catwalks are likely to,[189] but sports performances do not. Lord Justice Arnold argues that an improvisation could also be protected as a performance,[190] but there is currently no precedent for this. There is no requirement for reputation, notoriety, professional status, or goodwill to receive protection under performers' rights. Under this definition therefore, Pavis suggests that teachers, politicians, journalists and individuals sharing their videos on social media are performers and are legally entitled to control their performances.[191] This suggests that performers rights in video content used to generate a deepfake may be relevant.

However, the mere imitation of a performance is not actionable. Performers' rights only protect the *recording* of a performance and the copying of that recording, not the content of the recording.[192] Pavis believes that because AI systems used to generate deepfakes do not copy recordings of performances, they fall outside the scope of protection by performers' rights.[193] Consequently, deepfakes may not fall within the scope of these rights. Performers who are being displaced by deepfakes are currently not able to prevent developers, or those utilising this technology, from copying their likeness or performance in this way. As such, the Culture, Media and Sport Select Committee (CMSC) has concluded that 'the UK's patchwork of copyright, intellectual property and data protection legislation is failing to protect performers from the nefarious use of generative AI technologies, such as unauthorised voice cloning and deepfakes.'[194] It recommended that the Government improve protections for creatives to prevent misuse of their likeness and performances by generative AI. At a minimum, it advocated, this should involve bringing forward ratification of the Beijing Treaty on Audiovisual Performances.[195]

The Beijing Treaty[196] has been cited as one way of potentially addressing these concerns.[197] The international agreement came into force on 28 April 2020, providing intellectual property rights and certain moral rights in audiovisual performances, including performances given by actors, musicians, dancers and other performers whose work is featured in films, television programmes and other audiovisual recordings. The UK Government signed the Treaty in 2013 but did not implement it. Since leaving the European Union (EU) it has now committed to ratifying the Treaty.[198] UK law is already largely compliant but does not provide any exclusive rights for broadcasting and communication to the public for fixed audiovisual performances. This means that once a performer has agreed to their performance being incorporated in an audiovisual fixation, they do not have a statutory right to prevent it being broadcast or communicated to the public, or to receive remuneration for these uses.[199]

The UK Intellectual Property Office (IPO) initially launched a consultation on implementing the Beijing Treaty in 2021.[200] Respondents broadly supported the move, but views on how to do so varied.[201] A second call was launched to seek evidence on implementing new moral rights, economic rights and international reciprocity. This consultation ran until November 2023, then, in February 2024, the Government announced that it had reviewed the evidence but required more analysis.[202] Although it had initially estimated this work would be completed by 2024,[203] there is no clear timeline on if, when or how the Treaty will be ratified into UK law.[204]

Although the Treaty does not include specific provisions for audiovisual performers to protect their rights against deepfakes,[205] it can provide new moral rights to performers that may be relevant. The right to attribution would require that the performer be correctly identified, and the right to integrity would allow the performer to object to any distortion, mutilation or modification of their performance that would be prejudicial to their honour or reputation. UK law already provides these rights for live performances and performances in sound recordings,[206] but not for performances in audiovisual fixations. This would need to be amended to ratify the Treaty and could therefore potentially add to a performers' protection against deepfake in certain circumstances. However, it remains unclear whether these rights will be included, and if so to what extent the scope of the rights will be applicable. Indeed, the Government itself has accepted the limitations of performer's rights and the Beijing Treaty in dealing with the misuse of performers' likenesses.[207]

The CMSC has since affirmed that there is an urgent need for the UK to codify image rights to protect performers from the unauthorised use of their identity by generative AI tools, alongside protecting the general public from non-consensual exploitation of an individual's likeness.[208] It noted that the lack of protection against 'unauthorised digital imitations of people.'[209] Whilst, the Government has taken action to criminalise the generation of sexually explicit deepfakes, there remains 'a gap in protection' for non-criminal yet harmful uses of people's likeness.[210]

3.9 | Technical solutions

Technological solutions, such as increased use of detection and labelling tools, have been suggested to, at least in part, address some of the concerns raised by deepfakes.[211] Ofcom state that this will require action from all actors in the technology supply chain—from the developers that design AI models and tools, to the platforms that host this technology, through to the user-facing services providing spaces for deepfake content to be shared and amplified.[212] The CMSC noted that some industry initiatives are being introduced, such as by YouTube to implement stricter measures on AI-generated content.[213] Likewise, companies including Google, Meta, Microsoft, OpenAI, TikTok and X announced 'a set of commitments to deploy technology countering harmful AI-generated content meant to deceive voters.'[214] The Secretary of State for Science, Innovation and Technology has also pointed to working with industry to evaluate existing detection functions, develop deepfake watermarking tools, and embed ethical responsibility through safety-by-design.'[215]

However, this did not prevent the Grok AI chatbot on X being used to create and share demeaning sexual deepfakes of real people, including children.[216] Moreover, labelling deepfakes only attempts to address the harm of disinformation and does not reduce the harms of demeaning content or displacing workers. Furthermore, the reluctance of social media companies in working with the criminal justice system to disclose information contained on their sites, and their slow response in removing abusive content, makes doubtful of the reliability of such promises.[217] These issues cannot be solved through deepfake detection techniques and algorithms alone.[218] In particular, platforms should not be granted the power to determine which deepfakes are removed or remain online, as there is a clear conflict of interest; since they have a vested interest in content being shared.[219]

Recent developments under the Online Safety Act 2023, do now require that online services have duties to protect users' safety and puts the onus on platforms to remove certain content. Ofcom, the regulator for online safety, have stated that they will need to address the dissemination of some, but not all, types of deepfakes.[220] This is because the scope of the online safety regulation is limited, only obliging platforms to remove explicit deepfakes, and not any other unauthorised forms.[221] Campaigners have argued that the Ofcom guidance on these issues are inadequate, calling it 'ignorable.'[222] Moreover, they contend that there is a disproportionate focus on the costs and burden for technology companies, rather than a focus on the harm caused.[223]

A further limitation of technological solutions is the inherent bias of protecting marginalised groups; for example, deepfake detection tools do not always work for people with darker skin tones, particularly if the tools are not trained with data sets that include people of diverse ethnicities.[224]

There is also the risk that social media companies continue to do what they already do in relation to related laws, and that is to downstream the liability to users through the terms and conditions, which are rarely read or understood by the user.[225] Early warning signs of this can be seen in Stability AI's arguments in the Getty case, mentioned above.[226] Notice and takedown procedures currently allow users to request the removal of content that infringes their intellectual property rights, however, the law does not currently encompass deepfakes.

The above sections have reviewed the legal and policy landscape that may be applicable to unauthorised deepfake. The analysis has demonstrated that while some areas of law offer protection in specific circumstances, none adequately address the harms set out above. As the Alliance for Universal Digital Rights argues, legal redress is 'patchy at best.'[227] Therefore, this paper argues that this justifies the introduction of personality rights under UK law, discussed in the next section.

4 | NEW REGULATION OF DEEPFAKES

The patchwork of legal protection, together with the immediate amendments suggested to the Online Safety Act,[228] demonstrates that a technological specific law aimed at deepfakes will not adequately address the harms. Instead, the law should focus on what needs *protecting*, rather than what it needs protecting *against*. This means providing rights for a person's image and likeness, instead of trying to regulate the moving target of technology. The following section considers the theoretical justification for personality rights in light of the harms discussed above and the laws inadequacy to regulate those harms. It then makes a proposal for the position and scope of personality rights under UK law.

4.1 | Proposal for UK personality rights

Llewellyn's legislative theory reasons that the purpose of law lies in the need to resolve conflicts that occur within a group of people,[229] whereby the law provides a mechanism for these conflicts to be resolved. Accordingly, the conflict, or problem, relates to the 'mischief rule,' based on the principle that legislation is created to solve a problem, with the goal of suppressing the mischief and advancing the remedy.[230] It follows that regulation is drafted with the intention to address a problem that may occur in society, and remedy the issue to restore social order. Llewellyn explained that the fundamental purpose of law is the 'adjustment of people's behavior [so] that the society remains a society and gets enough energy unleashed and coordinated to keep on with its job as a society.'[231] For the present purposes, the 'mischiefs' are the harms demonstrated above. This section makes legislative proposals for addressing such harms in accordance with the mischief rule, underpinned by Llewellyn's legislative theory.

However, legislation alone is not enough. As demonstrated, the harms of deepfakes permeate across industries, exacerbate systemic issues of sexism, racism and misogyny whilst escalating challenges of misinformation and threats to the creative industries, conceptualised as 'an assemblage of differential tensions, comprised of interlinking and overlapping ruptures and continuities.'[232] Legislation is needed and technological interventions are required, but as Lord Tim-Clement-Jones states: 'even the combination of regulation and technology cannot deal with all the issues of misinformation, disinformation and deepfakery.'[233] The UK must adopt a holistic approach that includes legislative and technological interventions as well as educational and cultural actions to address the systemic issues that underpin and propel deepfake harms.

In terms of the legislation required, the regulatory framework needs to be clear, robust and flexible as the technology inevitably develops.[234] It must be centred around the consent of the victim, not the intent of the perpetrator, which can vary and be difficult to prove. Likewise, it must encapsulate all relevant parties, regulating those that generate the deepfake, those who possess or share it, as well as platforms, websites and applications that facilitate, generate, host or store deepfakes. The current UK law on explicit deepfakes should be expanded to encapsulate all these elements. Google argues that extending liability this far would disincentivise developers from designing creative tools for fear of being held liable as a co-creator of violative content.[235] However, developers must be held accountable for ensuring that the purpose of their applications does not cause harm. There is no legitimate reason for applications that 'undress' an image for example, and so, the harms far outweigh any possible benefits.

To address the full range of deepfake harms, instead of drafting technologically specific legislation which will become obsolete, legislating for a new personality right would be more effective and appropriate.

The All-Party Parliamentary Group on Music recommended the introduction of a personality right to safeguard creators and artists from misappropriation and false endorsement, protecting voice, image, name, and likeness.[236] In the UK consultation on AI and copyright, questions were asked in relation to digital replicas, such as to what extent would the approaches outlined in the consultation provide individuals with sufficient control over the use of their image and voice in AI outputs?[237] The responses to the consultation are currently unpublished;[238] however, some organisations and individuals have publicly shared their views. For example, Open AI said that it believed the UK already has legal protections that can address unauthorised digital replicas, including passing off, performers' rights, sound recording rights, and data protection laws, but suggested that targeted legislation could fill in any gaps.[239] Google argued that a personality right would be a threat to creative and free expression.[240] Researchers also note the importance of not restricting biographical and historical information, such as for the purpose of creating a biopic film which requires a replica of an individual.[241]

Equity has nevertheless called for the introduction of statutory image rights that restrict the unauthorised use of persona, which it believes is the 'most coherent and desirable solution.' Ninety-three percentage of their membership is in favour of new legal protections for performers so that a performance cannot be reproduced by AI without consent.[242]

Personality rights do already exist in other jurisdictions. For example, Guernsey protects personality rights, under the Image Rights (Bailiwick of Guernsey) Ordinance 2012, including voice, likeness, appearance, silhouette, face and mannerisms. Registration grants a property right that can be protected, licensed and assigned. There are limitations to this right, such as fair dealing for the purposes of research, news reporting, of the arts, or for educational purposes.[243] The deterrence effect of this legislation is questionable since Guernsey Police still warn of a rise in deepfake scams.[244] Perot suggests that the registration requirement is an unnecessary step that makes it harder for individuals to protect their persona, since failing to register would prevent them from having a cause of action.[245] The UK Online Safety Act 2023 and amendments of the UK Data (Use and Access) Bill extend to Guernsey now also making it illegal to create explicit deepfakes, as discussed above. Therefore, the proposal below recommends a personality right that does not need to be registered.

In India, a Bollywood singer, Arijit Singh, litigated the unauthorised cloning of his voice. The Bombay High Court recognised the protection of Singh's name, voice, vocal style and technique, mannerism, image, caricature, likeness and signature. Under the common law of India, personality and publicity rights are vested in celebrities and the unauthorised use of their name or other persona attributes.[246] The suit also raised a claim under statutory moral rights in Singh's performances.[247] The defendants were ordered to remove and block access to all infringing content.[248] This case shows that in India, in certain circumstances, celebrities who demonstrate goodwill are able to protect themselves against unauthorised deepfakes, and enforce those rights against the creators, disseminators and hosts. However, this law does not assist those unable to demonstrate celebrity status, leaving many individuals unprotected. The proposed personality right for UK law would apply to all persons, regardless of celebrity status.

In the USA, most States recognise a right of publicity or image rights to address the use of an individual's persona in commercial contexts, either through statutory or common law provisions.[249] Typically, these only apply in circumstances of advertising, merchandise, or for commercial purposes. The scope of the rights differs significantly between States, and many require commercial value in the individual's identity.[250] As a result, the US Copyright Office advocated that new federal legislation is urgently needed to address the harms that can be inflicted by non-commercial uses, including deepfake pornography. Likewise, existing federal laws, such as copyright and privacy, are too narrow to fully address the harm of deepfakes. Therefore, it concluded that the time has come to adopt a federal law against digital replicas, proposing a new right that extends protection to all individuals regardless of their commercial value of their identities.[251]

Most recently, Denmark has made a ground breaking proposal to reclassify a person's identity, through their face, voice, and physical characteristics, as a form of intellectual property. The proposals amend the Danish Copyright Act to establish a person's likeness as an enforceable asset, meaning that Danish citizens will soon be able to take legal action against deepfakes on this basis. Whilst little detail is known at the early stages of this development, it is a world first in taking steps to utilise the intellectual property framework to address the harms of deepfakes.[252] The proposed Bill has exceptions including imitations that are mainly expressions of caricature, satire, parody, pastiche, criticism of power, criticism of society, unless the imitation constitutes misinformation that can cause serious danger to the rights or essential interests of others. The proposal for personality rights under UK law also suggests including exceptions and could follow the Danish model for the scope of these limitations.

The new statutory right must be balanced with freedom of expression, which can be achieved through limitations, just as copyright provides the right to restrict the unauthorised use of a work[253] with specific exceptions.[254] Not all copyright exceptions would be required or appropriate, such as the making of temporary copies,[255] but certainly, criticism, review, quotation and news reporting would be relevant exceptions.[256]

Researchers have raised a second concern on the term of protection for personality rights, noting that in some jurisdiction's personality-based rights are perpetual, which some believe are excessive.[257] Equity argues that a new right should extend post-mortem, but not necessarily in perpetuity.[258]

To compare, copyright in an original work lasts for life of the creator plus 70 years,[259] and moral rights subsist as long as the copyright.[260] Performance rights exist for 50 years,[261] but this right only restricts the recording of a performance, therefore aligning with non-original copyright protection, such as that of sound-recording or film, which also lasts for 50 years.[262] The definition of original, in the context of copyright, relates to the expression of intellectual creation; to add the stamp of one's personal touch.[263] It follows that a right to personality would inevitably require one's own personal touch in order to be distinct from another's persona. Therefore, the new personality right should be aligned with original rights and subsist, along with copyright and moral rights, for 70 years after the death of the person. This also reflects user perceptions and expectations.[264]

A further concern is that individuals could be pressured into signing away any personality right to a dominant player due to inequality of bargaining power in the creative industries.[265] However, copyright is structured as a balancing tool between stakeholders for this precise purpose.[266] Utilising copyright principles, the law can enable the rightsholder to receive a reward that corresponds to a fair share of the revenue generated by the exploitation of their work.[267] Rights can be unwaivable and a statutory reward can be required in exchange for any transfer of rights, which presupposes that the ordinary working of the market is insufficient, and such protection is required for those who are inevitably in a weaker bargaining position at the point of transferring their rights.[268]

Like copyright, the right should arise automatically without the need for registration, avoiding the exclusions created under the Guernsey law. However, unlike a copyright work created in the course of employment,[269] the personality right must vest in the person and not the employer. Doing otherwise would conflict with a person's Human Rights[270] and not address the issues of HDTs.

Therefore, it is proposed that an automatic unwaivable personality right is introduced, subsisting in a person's voice, image, name, and likeness, regardless of commercial use, implemented through amendments to the CDPA 1988. The right should subsist for a term of 70 years after the death of the person and be limited by exceptions such as criticism, review, quotation.

In addition, other legal interventions are also required. Firstly, the Online Safety Act 2023 needs to be extended to include possession of an unauthorised deepfake. Nudification and 'undressing' apps should be banned, since there is no legitimate purpose for them other than to perpetuate and escalate misogynistic harms. Additionally, given the clear connection between violent pornography and physical violence, regulation should apply to unauthorised deepfakes that include gender-based violence and harmful stereotypes.

Secondly, for the proposed personality right and regulation of deepfakes to be effective, AI technology companies must be transparent about the input data used to train their AI models. This has not formed part of the UK Data Bill, despite widespread pushback and five rounds of amendments from the House of Lords attempting to include a transparency measure.[271]

Thirdly, further technological intervention is needed, such as requiring platforms and web-service providers to remove unauthorised deepfake content and content-hosting websites, as well as including digital replicas in their notice and take down policies.

Fourthly, although outside the scope of this article, it is acknowledged that educational and cultural interventions are also essential, as advocated for by Violence Against Women and Girls organisations.[272] This includes the allocation of resources and funding for school and community programmes for boys, to encourage healthy discussions about positive masculinity and counter misogynistic culture.[273]

5 | CONCLUSION

This paper has discussed the harms caused by deepfakes in three categories: disinformation, demeaning content and displacing creative workers. It then mapped the current UK law that may apply in certain circumstances to digital replicas. As such, this paper concludes that the harms caused by unauthorised deepfakes, together with the emerging threats of human digital twins, are not adequately addressed under current UK law and reform is needed. We are at a cross roads. We can regulate and steer AI technology in the direction of ethical new possibilities or let it lead us further down the path of the current and emerging harms into a world without control over the use of our own personas in the digital domain.

This paper acknowledges that legislative reform on its own is not enough to tackle the harms, but it is a foundational part of the holistic agenda required that must be supplemented by educational, cultural and technological intervention.

Still, the merging of personhood and technology, and the harms that this causes, expands the scope of the protection required for personality and property.[274] It therefore suggests the introduction of personality rights into UK law. It argues for an unwaivable, automatic personality right, embedded in the current copyright regime, aligned with the term of copyright protection and appropriate exceptions.

Whilst personality rights have been applied, to some degree, in other jurisdictions, and formed part of the reform discourse for some time, never has there been such a defined need to implement them. As Caroline Norton famously wrote to Queen Elizabeth in 1855: 'A very shallow reader of history might prove, that from time immemorial, changes in the laws of nations have been brought about by individual examples of oppression. Such examples cannot be unimportant, for they are, and ever will be, the little hinges on which the great doors of justice are made to turn.'[275] Deepfakes are the hinges on which to open the door of personality rights in the UK, for the protection against the harms of unauthorised digital replicas.

DATA AVAILABILITY STATEMENT

The author has nothing to report.

ORCID

Hayleigh Bosher https://orcid.org/0000-0002-4771-7469

ENDNOTES

[1] Andreas Kaplan, 'Artificial Intelligence, Social Media, and Fake News: Is This the End of Democracy?' In A.A. Gül, Y.D. Ertürk and P. Elmer (eds) *Digital Transformation in Communication and Media Studies* (University Press 2020).

[2] Ofcom, 'Deepfake Defences, Mitigating the Harms of Deceptive Deepfakes' (Ofcom July 2024) 4.

[3] Emily Zemler, ‘Randy Travis Releases His Second AI Song ‘Horses in Heaven’ (*Rolling Stone*, 31 January 2025) <https://www.rollingstone.com/music/music-country/randy-travis-horses-in-heaven-single-1235252432/> accessed 13 August 2025.

[4] Lucy O'Dair and Mark Taylor, ‘Deepfakes’ (2024) 30(8) CTLR 201–202, 202.

[5] ‘Copyright and Artificial Intelligence, Part 1: Digital Replicas’ (US Copyright Office July 2024) 4.

[6] Marie-Helen Maras and Alex Alexandrou, ‘Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos’ (2019) 23(3) EP 255–262, 256.

[7] Security Heroes ‘2023 State of Deepfakes, Realities, Threats, and Impact’ (Security Heroes 2023).

[8] Sensity, ‘The State of Deepfakes 2024’ (Sensity 2025) 5.

[9] Centre for Data Ethics and Innovation, ‘Deepfakes and Audiovisual Disinformation’ (CDEI 12 September 2019).

[10] Molly Blackall, ‘How Deepfake Videos Could Derail Democracy at the Next General Election’ (*inews*, 27 October 2023) <https://inews.co.uk/news/deepfake-videos-derail-democracy-next-general-election-2707917> accessed 13 August 2025.

[11] ‘Government Crackdown on Explicit Deepfakes’ (*Ministry of Justice*, 7 January 2025) <https://www.gov.uk/government/news/government-crackdown-on-explicit-deepfakes> accessed 13 August 2025.

[12] Bobby Chesney and Danielle Citron, ‘Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security’ (2019) 107 CLR 1753, 1757.

[13] Maras and Alexandrou (n 6).

[14] ‘Deepfake Abuse: Landscape Analysis, The Exponential Rise of Deepfake Abuse in 2023–2024’ (*My Image My Choice*, February 2024)16 <https://myimagemychoice.org/take-action/> accessed 13 August 2025.

[15] Santiago Lakatos, ‘A Revealing Picture’ (Raphika 8 December 2023) 1.

[16] Ofcom (n 2).

[17] Sensity (n 8), 9.

[18] Sarah Barrington, Emily Cooper and Hany Farid, ‘People are Poorly Equipped to Detect AI-Powered Voice Clones’ (2025) 15(11004) SR 1–9.

[19] ‘Copyright and Artificial Intelligence (n 5) §§ iii.

[20] Clemens Seibold, Eric Wisotzky, Arian Beckmann, Benjamin Kossack, Anna Hilsmann and Peter Eisert, ‘High-Quality Deepfakes Have a Heart!’ (2025) 4 FI 1–15.

[21] Zachariah Parry, ‘Digital Manipulation of Photographic Evidence: Defrauding the Courts One Thousand Words at a Time’ (2009) 81 JLTP 176.

[22] Ofcom, ‘Adults’ Media Use and Attitudes Report’ (Ofcom, 2022) 13.

[23] O'Dair and Taylor (n 4), 202.

[24] Maria de Arcos Tejerizo, ‘Digital Evidence and Fair Trial Rights at the International Criminal Court’ (2023) 36(3) Leiden JIL 749–769.

[25] Maras and Alexandrou (n 6).

[26] ‘Romance Fraudsters Break Hearts and Bank Balances with £92.8 m Lost in the UK Last Year’ (*City of London Police*, 2 December 2023) <https://www.cityoflondon.police.uk/news/city-of-london/news/2023/october/romance-fraudsters-break-hearts-and-bank-balances-with-92.8m-lost-in-the-uk-last-year/> accessed 14 August 2025.

[27] ‘Martin Lewis Felt “Sick” Seeing Deepfake Scam Ad on Facebook’ (*BBC*, 7 July 2023) <https://www.bbc.co.uk/news/uk-66130785> accessed 13 August 2025.

[28] Seb Butcher, ‘Disinformation, Generative AI and Why Our Laws Need Urgent Reform’ (2024) 30(4) CTLR 85-86.

[29] Steve Holland, ‘Fake “Biden” Robocall Tells New Hampshire Democrats to Stay Home’ (*Reuters*, 23 January 2024) <https://www.reuters.com/world/us/fake-biden-robo-call-tells-new-hampshire-voters-stay-home-2024-01-22/> accessed 13 August 2025.

[30] Marianna Spring, ‘Sadiq Khan Says Fake AI Audio of Him Nearly Led to Serious Disorder’ (*BBC*, 13 February 2024) <https://www.bbc.co.uk/news/uk-68146053> accessed 13 August 2025.

[31] Science, Innovation and Technology Committee, ‘Governance of Artificial Intelligence’ (HC 1769 28 May 2024) 10.

[32] Ofcom (n 2) 4.

[33] Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, 'The State of Deepfakes: Landscape, Threats, and Impact' (Deeptrace 2019) 1.

[34] Security Heroes (n 7).

[35] Deepfake Abuse (n 14) 3.

[36] Security Heroes (n 7).

[37] 'Protecting the Public from Abusive AI-Generated Content' (*Microsoft*, 5 November 2024) 9 <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Protecting-Against-Abusive-AI-Content-UK.pdf> accessed 14 August 2025.

[38] O'Dair and Taylor (n 4) 202.

[39] Deepfake Abuse (n 14), 11.

[40] 'AI-Generated Taylor Swift Porn Went Viral on Twitter. Here's How It Got There' (*404 Media*, 25 January 2024) <https://www.404media.co/ai-generated-taylor-swift-porn-twitter> accessed 14 August 2025.

[41] Deepfake Abuse (n 14), 6.

[42] Ibid, 7.

[43] College of Policing and National Police Chiefs' Council, 'Violence Against Women and Girls National Policing Statement 2024' (NPCC, July 2024) 20, 32-33.

[44] HL Deb Vol 836 Col 1777 8 March 2024.

[45] Deepfake Abuse (n 14), 7.

[46] Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell, Adrian Scott, *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery* (Routledge 2020).

[47] Laura Bates, *The New Age of Sexism, How the AI Revolution is Reinventing Misogyny* (Simon & Schuster 2025) 16

[48] Sarah Hooper, 'Girl Killed Herself When Bullies Shared Fake Nudes of Her' (*Metro*, 24 January 2024) <https://metro.co.uk/2024/01/24/teen-took-life-online-bullying-shared-fake-nudes-20162284/> accessed 14 August 2025.

[49] Jo-Ann Pattinson and Subhajit Basu, 'Can the Law Stop Internet Bots from Undressing You?' (*The Conversation*, 6 November 2020) <https://theconversation.com/can-the-law-stop-internet-bots-from-undressing-you-149056> accessed 14 August 2025.

[50] Deepfake Abuse (n 14) 11.

[51] Ofcom (n 2).

[52] 'Children's Commissioner Calls for Immediate Ban of AI Apps that Enable 'Deepfake' Sexual Abuse of Children (*Children's Commissioner*, 28 April 2025) <https://www.childrenscommissioner.gov.uk/news-and-blogs/press-notice-childrens-commissioner-calls-for-immediate-ban-of-ai-apps-that-enable-deepfake-sexual-abuse-of-children/> accessed 14 August 2025.

[53] HL Deb Vol 845 30 April 2025.

[54] Learn More About Meta AI on Ray-Ban Meta Glasses (*Meta*) <https://www.meta.com/en-gb/help/ai-glasses/326686793146045/> accessed 13 August 2025.

[55] Baroness Bertin, 'Creating a Safer World—The Challenge of Regulating Online Pornography' (DSIT February 2025) 36.

[56] Joanne Upton, Alya Hazell, Rachel Abbott and Kate Pilling, 'The Relationship Between Pornography Use and Harmful Sexual Attitudes and Behaviours: Literature Review' (Women and Equalities Unit 2021) 5.4.

[57] Julia Hörnle, 'Deepfakes and the Law: Why Britain Needs Stronger Protections Against Technology-Facilitated Abuse' (*Queen Mary University of London*, 23 January 2025) <https://www.qmul.ac.uk/media/news/2025/humanities-and-social-sciences/hss/deepfakes-and-the-law-why-britain-needs-stronger-protections-against-technology-facilitated-abuse.html> accessed 13 August 2025.

[58] Marc Tran, 'Combatting Gender Privilege and Recognizing a Woman's Right to Privacy in Public Spaces: Arguments to Criminalize Catcalling and Creepshots' (2015) 26(2) Hastings WLJ 185, 197; Fiona Vera-Gray, Clare McGlynn, Ibad Kureshi and Kate Butterby, 'Sexual Violence as a Sexual Script in Mainstream Online Pornography' (2021) 61(5) British JC 1243–1260.

[59] College of Policing and National Police Chiefs' Council (n 43), 26.

[60] Elish Angiolini, 'Angiolini Inquiry Report Part 1' (HC 530 29 February 2024) 2.65, 2.69.

[61] Bates (n 47), 53.

[62] Benjamin Jacobsen and Jill Simpson, 'The Tensions of Deepfakes' (2023) 27(6) iCS 1095–1109, 1100.

[63] Colin Stutz, 'The Fake Drake AI Song Earned Millions of Streams—But Will Anyone Get Paid?' (*Billboard*, 19 April 2023) <https://www.billboard.com/pro/fake-drake-ai-song-earned-millions-streams-get-paid/> accessed 13 August 2025.

[64] Bill Donahue, 'Tupac Shakur's Estate Threatens to Sue Drake Over Diss Track Featuring AI-Generated Tupac Voice' (*Billboard*, 24 April 2024) <https://www.billboard.com/pro/tupac-shakur-estate-drake-diss-track-ai-generated-voice/> accessed 13 August 2025.

[65] Equity, Stop AI Stealing the Show <https://www.equity.org.uk/campaigns-policy/stop-ai-stealing-the-show> accessed 13 August 2025.

[66] Nick Bond, 'Disney Movie 'Prom Pact' Freaks Out Audiences With 'Horrendous' AI Extras' (*New York Post*, 15 October 2023) <https://nypost.com/2023/10/15/disneys-prom-pact-has-audiences-cringing-at-ai-actors/> accessed 13 August 2025.

[67] Cade Metz, 'What Do You Do When A.I. Takes Your Voice?' (*The New York Times*, 16 May 2024) <https://www.nytimes.com/2024/05/16/technology/ai-voice-clone-lawsuit.html> accessed 13 August 2025.

[68] Ed Nightingale, 'Baldur's Gate 3 Actors Reveal the Darker Side of Success Fuelled by AI Voice Cloning' (*Eurogamer*, 12 April 2024) <https://www.eurogamer.net/baldurs-gate-3-actors-reveal-the-darker-side-of-success-fuelled-by-ai-voice-cloning> accessed 13 August 2025.

[69] 'AI Cloning of Celebrity Voices Outpacing the Law Experts Warn' (*The Guardian*, 19 November 2024) <https://www.theguardian.com/technology/2024/nov/19/ai-cloning-of-celebrity-voices-outpacing-the-law-experts-warn> accessed 13 August 2025.

[70] Bob Piascik, John Vickers, Dave Lowry, Steve Scotti, Jeff Stewart, Anthony Calomino, 'Technology Area 12: Materials, Structures, Mechanical Systems, and Manufacturing Road Map' (NASA 2010) 15–88.

[71] AWS IoT TwinMaker <https://aws.amazon.com/iot-twinmaker/> accessed 13 August 2025.

[72] Yujia Lin, Liming Chen, Aftab Ali, Christopher Nugent, Ian Cleland, Rongyang Li, Jianguo Ding and Huansheng Ning, 'Human Digital Twin: A Survey' (2024) (13)131 JCCASA 1–21.

[73] Michael Miller and Emily Spatz, 'A Unified View of a Human Digital Twin' (2022) 4(1) HISI 23–33, 14.

[74] Neeraj Kavan Chakshu, Igor Sazonov and Perumal Nithiarasu, 'Towards Enabling a Cardiovascular Digital Twin for Human Systemic Circulation Using Inverse Analysis' (2021) 20(2) BMM 449–465.

[75] Barricelli BR, Casiraghi E, Gliozzo J, Petrini A, Valtolina S (2020) Human Digital Twin for Fitness Management (2020) 8 IEEE A 26637–26664.

[76] See for example, https://www.persona-institut.de/so-optimieren-digitale-zwillinge-recruiting-personalentwicklung-und-organisation/

[77] Saul Davila-Gonzalez and Sergio Martin, 'Human Digital Twin in Industry 5.0: A Holistic Approach to Worker Safety and Well-Being through Advanced AI and Emotional Analytics' (2024) (24)655 Sensors 1–20, 4.

[78] 'Talent Intelligence to Talent Advantage: Eightfold AI Revolutionizes HR through Agentic AI' (*Eightfold AI*, 8 May 2025) <https://www.prnewswire.com/news-releases/talent-intelligence-to-talent-advantage-eightfold-ai-revolutionizes-hr-through-agentic-ai-302449233.html> accessed 13 August 2025.

[79] Lin, Chen, Ali and other (n 72), 1.

[80] Copyright, Designs and Patents Act (CDPA) 1988, s11.

[81] Davila-Gonzalez and Martin (n 77), 17.

[82] Talya Deibel, 'Demarcation Problems in Law and Neurotechnology: Persons, Cyborgs and Neurohackers' [2025] IRLCT 1–20, 14.

[83] *Reckitt & Colman Products Ltd v Borden Inc (Jif Lemon)* [1990] 1 WLR 481 HL.

[84] Emmanuel Oke, 'Image Rights and Passing Off: Should Reputation be Enough for Celebrities to Succeed in English Courts?' (2020) 15(1) JIPLP 49-54.

[85] *Robyn Rihanna Fenty, Roraj Trade LLC, Combermere Entertainment Properties LLC* v *Arcadia Group Brands Limited (T/A Topshop), Top Shop/Top Man Limited* [2013] EWHC 2310 (Ch) 55.

[86] Emma Perot, 'Anticipating AI: A Partial Solution to Image Rights Protection for Performers' (2024) 46(7) EIPR 407–418, 414.

[87] *Robyn Rihanna Fenty, Roraj Trade LLC* (n 85), 55.

[88] [1977] FSR 62, 65.

[89] [1977] FSR 67-68.

[90] [2003] EWCA Civ 423.

[91] Stuart Heritage, 'Behind the Scenes of TV's First Deep Fake Comedy: "None of it is Illegal. Everything is Silly" (*The Guardian*, 9 January 2023) <https://www.theguardian.com/tv-and-radio/2023/jan/09/deep-fake-neighbour-wars-interview-itvx-comedy> accessed 13 August 2025.

[92] Trade Marks Act 1994, s1.

[93] UK00002645895.

[94] Stuart Heritage (n 91), s1(1)(b).

[95] UK00900895359.

[96] 30/10/2023, R 1266/2023-4, Weergave Van Het Gezicht Van Een Persoon (fig).

[97] Human Rights Act 1988; European Convention of Human Rights, Art 8.

[98] *Coco* v *Clark* [1969] RPC 41; *Campbell* v *MGN Ltd* [2002] EMLR 30.

[99] *Murray* v *Big Pictures* (UK) Ltd [2008] EWCA Civ 446.

[100] *Stoute and another* v *News Group Newspapers Ltd* [2023] EWCA Civ 523.

[101] *Seager* v *Copydex Ltd*. (1967) 1 WLR 923.

[102] Data Protection Act 2018, s10-11.

[103] Ibid, s 46-48.

[104] Michael Henry (ed), *International Privacy, Publicity and Personality Laws* (Butterworths 2001).

[105] Ronan Deazley, 'Introducing Publicity Rights–Breach of Confidence, the Photograph and the Commodifying the Image' (2003) 54(2) NILQ 99–117, 113, 115.

[106] *Sim* v *Stretch* (1936) [1936] 2 All ER 1237.

[107] Defamation Act 2013, s1(1).

[108] Defamation and Malicious Publication (Scotland) Act 2021.

[109] *Lachaux* v *Independent Print* [2019] UKSC 27.

[110] Matthew Lavy and Iain Munro, 'Liability for Economic Harm' in Matt Hervey and Matthew Lavy (eds) *The Law of Artificial Intelligence* (Sweet and Maxwell 2021) 177.

[111] 'Australian Mayor Abandons World-First ChatGPT Lawsuit' (*The Sunday Morning Herald*, 12 February 2024) <https://www.smh.com.au/technology/australian-mayor-abandons-world-first-chatgpt-lawsuit-20240209-p5f3nf.html> accessed 13 August 2025.

[112] *Norwich Pharmacal* v *Commissioners of Customs and Excise* [1974] AC 133.

[113] Daniel Shaw and Mollie Jackson, 'The Defamation Act 2013—10 Years Later' (2024) 29(3) CL 110–131, 121.

[114] Data Protection Act 2018 (n 102), s5(3).

[115] [2006] 3 All ER 336.

[116] Lavy and Munro (n 110), 180.

[117] Security Heroes (n 7).

[118] Henry, McGlynn, Flynn and others (n 46), Chapter 4.

[119] Criminal Justice and Court Act 2015, s33.

[120] UK Home Office, 'Threats to Disclose Private Sexual Photographs and Films' (UK Home Office July 2022).

[121] 'Upskirting: Know Your Rights' (*Ministry of Justice*, 11 February 2019) <https://www.gov.uk/government/news/upskirting-know-your-rights> accessed 13 August 2025.

[122] 'Sharing Photographs or Film of People in an Intimate State' (*College of Policing*, 15 May 2024) <https://www.college.police.uk/guidance/sharing-photographs-of-people-intimate-state> accessed 13 August 2025.

[123] Online Safety Act 2023, amending the Sexual Offences Act 2003, s66B.

[124] Ibid, s66B(10)(b).

[125] Deepfake Abuse (n 14), 3.

[126] CDPA 1988, s107(4)(b).

[127] Sharing Photographs or Film of People in an Intimate State (n 122).

[128] Bates (n 47), 37.

[129] Press release: Ministry of Justice and Alex Davies-Jones MP Published 7 January 2025 Government crackdown on explicit deepfakes <https://www.gov.uk/government/news/government-crackdown-on-explicit-deepfakes> accessed 3 March 2026.

[130] HC Deb 7 January 2025 vol 759 col 68WS.

[131] Clare McGlynn, 'Deepfake Porn: Why we Need to Make it a Crime to Create it, Not Just Share it' (*The Conversation*, 9 April 2024) <https://theconversation.com/deepfake-porn-why-we-need-to-make-it-a-crime-to-create-it-not-just-share-it-227177> accessed 14 August 2025.

[132] Baroness Bertin, 'Creating a Safer World—The Challenge of Regulating Online Pornography' (DSIT February 2025) 36.

[133] 'Government's Refusal to Act on Image-Based Sexual Abuse A devastating Letdown' (*End Violence Against Women*, 20 May 2025) <https://www.endviolenceagainstwomen.org.uk/governments-refusal-to-act-on-image-based-sexual-abuse-a-devastating-letdown/> accessed 14 August 2025.

[134] Protection of Children Act 1978; s 160 of the Criminal Justice Act 1988.

[135] Cyberflashing is where a person sends a photo of genitals without permission, which is illegal under s66A of the Sexual Offences Act 2003, inserted by the Online Safety Act 2023. Deepfake cyberflashing, by extension, is that act of sending deepfake genitals without permission, this is not currently regulated.

[136] Clare McGlynn, 'Cyberflashing: Consent, Reform and the Criminal Law' (2022) 86(5) JCL 336–352, 92.

[137] Science, Innovation and Technology Select Committee, 'Governance of Artificial Intelligence: Government Response' (HC 591 10 January 2025) 149–150.

[138] Press release: Ministry of Justice and Alex Davies (n 129).

[139] Crime and Policing Bill 2025.

[140] 'Better Protection for Victims Thanks to New Law on Sexually Explicit Deepfakes' (*Ministry of Justice*, 22 January 2025) <https://www.gov.uk/government/news/better-protection-for-victims-thanks-to-new-law-on-sexually-explicit-deepfakes> accessed 14 August 2025.

[141] Women and Equalities Committee, 'Tackling Non-Consensual Intimate Image Abuse' (HC 336 5 March 2025) 134.

[142] Ibid, 136.

[143] Women and Equalities Committee (n 141) 19, 3.

[144] Lucy Morgan, 'Survivors Have Bravely Shared Their Experiences of Image-Based Abuse—Why Won't the UK Government Listen? (*Glamour*, 20 May 2025) <https://www.glamourmagazine.co.uk/article/women-equalities-committee-image-based-abuse-government> accessed 14 August 2025.

[145] Laura Bliss, 'The Protection from Harassment Act 1997: Failures by the Criminal Justice System in a Social Media Age' (2019) 83 JCL 217, 227.

[146] College of Policing and National Police Chiefs' Council (n 43), 27.

[147] Official Statistics, 'Crime Outcomes in England and Wales 2023 to 2024' (*Home Office*, 30 January 2025) <https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2023-to-2024/crime-outcomes-in-england-and-wales-2023-to-2024#Section 2> accessed 14 August 2025.

[148] SITC, 'Governance of Artificial Intelligence: Government Response' (HC 591 10 January 2025) 15.

[149] 'Stalking and Harassment' (*CPS*, 23 May 2018) <https://www.cps.gov.uk/legal-guidance/stalking-or-harassment> accessed 13 August 2025.

[150] Protection from Harassment Act 1997, s2A(3)(c)(i)-(ii).

[151] Ibid, s2A(3).

[152] College of Policing and National Police Chiefs' Council (n 43), 7.

[153] Online Safety Act 2023, s179.

[154] Fraud Act 2006, s2.

[155] Dan Wyatt, Chris Whitehouse and Olivia Dhein, 'AI and Fraud—The New Frontier for Disputes?' (2024) (174) 8094 NLJ 17.

[156] Signicat, 'The Battle Against AI-Driven Identity Fraud' (Signicat 2024) 4.

[157] EWHC 1198 (Ch).

[158] Gabriella Swerling, 'Family Lawyer Warns of "deepfake" Evidence Being Used in the Courts' (*The Telegraph*, 1 February 2020) <https://www.telegraph.co.uk/news/2020/01/31/deepfake-audio-used-custody-battle-lawyer-reveals-doctored-evidence/> accessed 14 August 2025.

[159] Maras and Alexandrou (n 13), 255.

[160] Science, Innovation and Technology Committee (n 31), 238.

[161] Ibid, 154.

[162] Ibid, 155.

[163] Government response to the House of Lords Communications and Digital Committee report on 'The future of news' (January 2025) 9.

[164] CDPA 1988, s16 and s1.

[165] Laddie, Prescott and Vitoria, *The Modern Law of Copyright and Designs* (Butterworths 2011) 1.9.

[166] *HRH The Duchess of Sussex Claimant* v *Associated Newspapers Limited* [2021] EWCA Civ 1810.

[167] CDPA, 1988, Chapter VI.

[168] Ibid., s96(1).

[169] Ibid, s11(1).

[170] UK IPO, *Copyright and Artificial Intelligence* (UK IPO 17 December 2024).

[171] CDPA 1988, s16.

[172] Ibid, Chapter III.

[173] *Getty Images US Inc* v *Stability AI Ltd* [2025] EWHC 38 (Ch). Now under appeal *Getty Images (US) Inc & Ors v Stability AI Ltd (Re Form of Order)* [2025] EWHC 3343 (Ch) (16 December 2025). See also Bosher H., Copyright Infringement in AI Models: Statutory interpretation, Memorisation and Metaphors in *Getty Images* and *GEMA* (2026) 48(4) E.I.P.R, 1-26.

[174] UK IPO, *Copyright and Artificial Intelligence* (n 170).

[175] CDPA 1988, s 16(3)(a).

[176] *Ladbroke (Football)* v *Hill (William) (Football)* [1964] 1 WLR 273.

[177] *Newspaper Licensing Agency Ltd (NLA)* v *Marks and Spencer Plc* [2001] 3 WLR 290, 19.

[178] *Sheeran & Ors* v *Chokri & Ors* [2022] EWHC 827 (Ch), 206(2).

[179] CDPA 1988, s24.

[180] Ibid, s107(1)(a), s107(1)(e).

[181] Ibid, s107(2).

[182] Kinnier-Wilson J., 'Copyright: Criminal Copyright Infringement—s 107 and 110 CPDA 1988—Copyright in a Photocopy' (1994) 16(11) EIPR 217–248, 295.

[183] *Thames & Hudson Ltd* v *Design and Artists Copyright Society Ltd Times*, August 10, 1994 (Ch D).

[184] Eleonora Rosati, 'Infringing AI: Liability for AI-Generated Outputs under International, EU, and UK Copyright Law' (2024) EJRR 1–25, 24.

[185] *Getty Images US Inc* v *Stability AI Ltd* [2025] EWHC 38 (Ch).

[186] Ibid., 603-4.

[187] CDPA 1988, Part II.

[188] Ibid, s180(2).

[189] Mathilde Pavis, 'Runway Models, Runway Performers? Unravelling the Ashby Jurisprudence Under UK Law' (2018) 13(11) JIPLP 867–877.

[190] Richard Arnold, *Performers Rights* (Sweet & Maxwell 2021).

[191] Mathilde Pavis, 'Rebalancing Our Regulatory Response to Deepfakes with Performers' Rights (2021) 27(4) The International Journal of Research into New Media Technologies 974–998, 986.

[192] CDPA 1988, s 180.

[193] Pavis (n 192).

[194] CMSC, 'British Film and High-End Television' (HC 328, 10 April 2025) 57.

[195] CMSC, 'Connected Tech: AI and Creative Technology' (HC 1643 30 August 2023) 62.

[196] The Beijing Treaty on Audiovisual Performances 2012 WIPO TRT/BEIJING/001.

[197] CMSC (n 195), 60.

[198] CMSC, 'Government Response to the Committee's Eleventh Report of Session 2022-23 Culture, Media and Sport Committee, Connected Tech: AI and Creative Technology' (HC 441 11 January 2024) 6.

[199] Beijing Treaty, Art 11.

[200] Beijing Treaty on Audiovisual Performances: Call for Views (23 April 2021) <https://www.gov.uk/government/consultations/beijing-treaty-on-audiovisual-performances-call-for-views/beijing-treaty-on-audiovisual-performances-call-for-views> accessed 14 August 2025.

[201] Summary of responses <https://www.gov.uk/government/consultations/beijing-treaty-on-audiovisual-performances/consultation-on-the-options-for-implementing-the-beijing-treaty-on-audiovisual-performances> accessed 14 August 2025.

[202] Beijing Treaty Consultation (*UK IPO*, 7 February 2024) <https://www.gov.uk/government/consultations/beijing-treaty-on-audiovisual-performances> accessed 13 August 2025.

[203] Government Consults on Implementation of Beijing Treaty on Audiovisual Performances (*UK IPO*, 14 September 2023) <https://www.gov.uk/government/news/government-consults-on-implementation-of-beijing-treaty-on-audiovisual-performances> accessed 13 August 2025.

[204] Lois Jeary and Devyani Gajjar, 'Artificial Intelligence and New Technology in Creative Industries' (*POST*, 7 October 2024) <https://post.parliament.uk/artificial-intelligence-and-new-technology-in-creative-industries/#_edn38> accessed 13 August 2025.

[205] CMSC (n 198), 6.

[206] CDPA 1988, Chap 3.

[207] CMSC (n 198), 6.

[208] CMSC (n 194), Equity (BF20019).

[209] Ibid., 456 Q21.

[210] Ibid, referencing Trades Union Congress, Artificial Intelligence for Creative Workers: A TUC Manifesto, 3 March 2025, 15.

[211] Ofcom (n 2), 3.

[212] Ibid, 5.

[213] CMSC (n 194), 6.

[214] Science, Innovation and Technology Committee (n 31), 241.

[215] Secretary of State DSIT Letter to Dear Baroness Stowell (17 April 2024) <https://committees.parliament.uk/publications/44576/documents/221444/default/> accessed 14 August 2025.

[216] Ofcom update: Investigation into X, and scope of the Online Safety Act (3 February 2026) <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/investigation-into-x-and-scope-of-the-online-safety-act> accessed 3 March 2026.

[217] Bliss (n 145), 228.

[218] Jacobsen and Simpson (n 62), 1106.

[219] Hayleigh Bosher and Sevil Yesiloglu, 'An Analysis of the Fundamental Tensions Between Copyright and Social Media: The Legal Implications of Sharing Images on Instagram' (2018) 33(2) IRLCT 164-186.

[220] Ofcom (n 2), 3.

[221] Women and Equalities Committee (n 141), 19.

[222] 'Responding to Ofcom's 'Violence Against Women and Girls' Guidance for the OSA' (*Glitch*, 20 May 2025) <https://glitchcharity.co.uk/blog/ofcom-vawg-guidance-response> accessed 14 August 2025.

[223] Open letter from End Violence Against Women to Dame Melanie Dawes Chief Executive Ofcom (23 February 2024) <https://www.endviolenceagainstwomen.org.uk/ofcom-blocking-a-safer-internet-for-women-vawg-experts-warn> accessed 14 August 2025.

[224] Bates (n 47), 47.

[225] Bosher and Sevil Yesiloglu (n 219), 186.

[226] *Getty Images US Inc* v *Stability AI Ltd* (n 185).

[227] 'Deepfake Image-Based Sexual Abuse, Tech-Facilitated Sexual Exploitation and the Law (*Alliance for Universal Digital Rights*, 24 January 2024) <https://audri.org/new-research-brief-deepfake-image-based-sexual-abuse-tech-facilitated-sexual-exploitation-and-the-law/> accessed 14 August 2025.

[228] Ofcom update: Investigation into X, and scope of the Online Safety Act (3 February 2026) <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/investigation-into-x-and-scope-of-the-online-safety-act> accessed 3 March 2026.

[229] Karl Llewellyn, 'The Normative, The Legal and the Law-Jobs: The Problem of Juristic Method' (1940) 49(8) YLJ 1355–1400.

[230] *Warburton* v *Loveland* (1832) 5 ER 499, 22.

[231] Llewellyn (n 229), 1373.

[232] Jacobsen and Simpson (n 62), 1106.

[233] Tim Clement-Jones, *Living with the Algorithm, Servant or Master? AI Governance and Policy for the Future* (Unicorn 2024) 45.

[234] Butcher (n 28).

[235] Google Response to UK IPO AI Consultation, 13 <https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Google_response_to_UK_Copyright__AI_Consultation_February_2025_hLpZUuW.pdf> accessed 14 August 2025.

[236] APPG on Music, *Artificial Intelligence and the Music Industry—Master or Servant?* (UK Music 2024) 18.

[237] UK IPO, *Copyright and Artificial Intelligence* (*n* 170), question 43.

[238] Copyright and Artificial Intelligence Statement of Progress Under Section 137 Data (Use and Access) Act (15 December 2025) < https://www.gov.uk/government/publications/copyright-and-artificial-intelligence-progress-report/copyright-and-artificial-intelligence-statement-of-progress-under-section-137-data-use-and-access-act> accessed 3 March 2026.

[239] Open AI Response to UK IPO AI Consultation, 16 (2 April 2025) < https://openai.com/global-affairs/response-to-uk-copyright-consultation/> accessed 3 March 2026.

[240] Google Response to UK IPO AI Consultation, 13 <https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Google_response_to_UK_Copyright__AI_Consultation_February_2025_hLpZUuW.pdf> accessed 14 August 2025.

[241] CREATe, Copyright and AI: Response by the CREATe Centre to the UK Government's Consultation (CREATe Working Paper 2025/2) 41.

[242] Equity (n 65).

[243] Guernsey protects personality rights, under the Image Rights (Bailiwick of Guernsey) Ordinance 2012, s31.

[244] 'Safer Internet Day 2025' (*Guernsey Police*, 11 February 2025) <https://www.guernsey.police.uk/SaferInternetDay25> accessed 14 August 2025.

[245] Perot (n 86) 407–418, 416.

[246] *Arijit Singh* v *Codible Ventures LLP and Ors*, Interim Application (L) No.23560 of 2024 in Com IPR Suit (L) No.23443 of 26 July 2024, 7, 16.

[247] Indian Copyright Act 1957, s38-B; Ibid, 3.

[248] Ibid, 21.

[249] J. Thomas Mccarthy and Roger E. Schechter, *The Rights of Publicity and Privacy* (Thomson Reuters 2024) 5:62.

[250] US Copyright Office, 'Copyright and Artificial Intelligence, Part 1: Digital Replicas' (US Copyright Office July 2024) 23.

[251] Ibid, 29.

[252] Giovana Fleck Denmark Leads EU Push to Copyright Faces in Fight Against Deepfakes (7 October 2025) <https://www.techpolicy.press/denmark-leads-eu-push-to-copyright-faces-in-fight-against-deepfakes/> accessed 3 March 2026.

[253] CDPA 1988, s16.

[254] Ibid, Chapter III.

[255] Ibid, s28A.

[256] Ibid, s30.

[257] CREATe, Copyright and AI: Response by the CREATe Centre to the UK Government's Consultation (CREATe Working Paper 2025/2) 42.

[258] Equity (n 65).

[259] CDPA 1988, s12.

[260] Ibid, s86(1).

[261] Ibid, s191(2).

[262] Ibid, s13.

[263] *THJ Systems Limited & Anor* v *Daniel Sheridan & Anor* [2023] EWCA Civ 1354, 16.

[264] Edina Harbinja, Tila Morse and Lillian Edwards, 'Digital Remains and Post-Mortem Privacy in the UK: What do Users Want?' [2025] IRLCT, 1–24.

[265] CREATe, Copyright and AI: Response by the CREATe Centre to the UK Government's Consultation (CREATe Working Paper 2025/2) 42.

[266] Abraham Drassinower, 'From Distribution to Dialogue: Remarks on the Concept of Balance in Copyright Law' (2009) 34 JCL 991–1007, 992.

[267] Laddie, Prescott and Vitoria, *The Modern Law of Copyright and Designs* (Butterworths 2011) 2163.

[268] Hayleigh Bosher, 'The UK Economics of Music Streaming Inquiry' (2022) 33(2) ELR 50–56.

[269] CDPA 1988, s11.

[270] Human Rights Act 1998, Art 5, 8 and 10.

[271] Dan Milmo and Raphael Boyd, House of Lords pushes back against government's AI plans (The Guardian, 12 May 2025) https://www.theguardian.com/technology/2025/may/12/house-of-lords-pushes-back-ai-plans-data-bill accessed 3 March 2026.

[272] Morgan (n 144).

[273] Baroness Bertin, 'Creating a Safer World - The Challenge of Regulating Online Pornography' (DSIT February 2025) 13.

[274] Deibel (n 82).

[275] Caroline Norton Letter to the Queen (2 June 1855) 133 <https://digital.library.upenn.edu/women/norton/alttq/alttq.html> accessed 14 August 2025.

AUTHOR BIOGRAPHY

Dr Hayleigh Bosher, Brunel University of London. Hayleigh is a Reader in Intellectual Property Law at Brunel, University of London. Hayleigh was awarded the British Academy Researcher-led Innovation Fellowships 2024–25 for her project 'The Future of the UK Music Industry: Exploring Policy and Practice,' in partnership with the Department for Digital, Culture, Media and Sport (DCMS). Hayleigh's research focuses on copyright and related laws in the creative industries, particularly relating to music, social media, and artificial intelligence. Her research always involves public, policy and industry engagement, with an emphasis on helping creators understand their rights whilst at the same time ensuring that those rights are fairly balanced and adequately supported by law. As such, she is widely published in academic peer-reviewed journals, in the press, and has responded to a number

of policy inquiries at international and national level. Her recent book; Copyright in the Music Industry, is accompanied with a playlist and podcast which she produces and co-hosts with Jules O'Riordan (AKA Judge Jules). She appeared before the DCMS Select Committee in relation to their Inquiry on the Economics of Music Streaming, the Science, Innovation and Technology Select Committee for their Inquiry on the Governance of Artificial Intelligence and the House of Lords Communications and Digital Committee on Large Language Models. Hayleigh is well-recognised in the field of intellectual property law, in particular copyright law and policy in the creative industries, she has attained an international reputation in the field of music copyright in particular. Her work in this area has been cited extensively in academic, practitioner and policy outputs and she is regularly interviewed by numerous national and international media outlets, including the BBC, ITV, Sky News, Channel 5 News and The Guardian, The Times and The Wall Street Journal. Hayleigh is a member of the UK Intellectual Property Office Research Experts Advisory Group, the Centre for Artificial Intelligence: Social and Digital Innovation, and the Research Centre for Law, Economics and Finance at Brunel, and a Visiting Research Fellow at the Centre for Intellectual Property, Policy and Management. Hayleigh joined Brunel in 2018, having previously held positions at Coventry University, The University of the Arts London and the Academy of Digital Entertainment, Breda University (Netherlands). Hayleigh holds a PhD in Copyright Law from Bournemouth University, under the Vice Chancellor's Scholarship Award.

How to cite this article: Bosher, H. (2026). 'Do Deepfakes, Digital Replicas and Human Digital Twins Justify Personality Rights?' *The Journal of World Intellectual Property*, 1–28. https://doi.org/10.1111/jwip.70020