Is This Video Real? The Principal Mischief of Deepfakes and How the Lanham Act Can Address It

QUENTIN J. ULLRICH[*]

This Note argues that the false association cause of action under Section 43(a)(1)(A) of the Lanham Act is well-suited for addressing problems posed by deepfakes, and outlines for practitioners the mechanics of such a cause of action. A "deepfake," which is a portmanteau of "deep learning" and "fake," is a digitally manipulated, often highly realistic video that substitutes the likeness of one person with that of another. Due to the way they deceive their viewers, deepfakes pose a threat to privacy, democracy, and individual reputations. Existing scholarship has focused on defamation, privacy tort, copyright, regulatory, and criminal approaches to the problems raised by deepfakes. These legal approaches may at times be successful at penalizing the creators of pernicious deepfakes, but they are not based on a theory of consumer confusion, which this Note argues is the principal mischief posed by deepfakes. Further, since deepfakes are often uploaded anonymously and the only effective remedy is against website owners, certain of these approaches are frustrated by the Communications Decency Act's immunization of website owners from liability for torts with a "publication" element. Hence, this Note proposes that the law of false association, which is principally concerned with consumer confusion, is best suited for addressing deepfakes. Importantly, a Lanham Act cause of action would allow victims of deepfakes to sue website owners under a theory of contributory infringement, because the Communications Decency Act does not immunize website owners from intellectual property claims.

INTRODUCTION

It is October of an election year, and there is an inflammatory video circulating of one of the presidential candidates criticizing voters in key swing states.[1] Is it real, or is it a deepfake? Deepfakes are digitally manipulated videos that substitute the likeness of one individual with that of another, or otherwise alter someone's likeness.[2] These videos, often uploaded to the internet anonymously, can appear highly realistic due to advances in video editing techniques, machine learning, and artificial intelligence. As a result, deepfakes have a high propensity to mislead their viewers. Although prominent social media sites such as Twitter have implemented policies forbidding misleading deepfakes,[3] other, more fringe, websites may either willfully ignore pernicious deepfakes or encourage their circulation. Even if a video is identified as fake, some websites may refuse to take the video down, and the target of the video—such as the hypothetical presidential candidate discussed above—may choose to resort to the courts for compensation, an injunction, or greater public recognition of the fakery.

This Note argues that a false association cause of action under Section 43(a)(1)(A) of the Lanham Act is well-suited for addressing deepfakes due to its focus on confusion and the fact the Communications Decency Act (CDA) does not block false association claims against website owners.[4] Section 43(a)(1)(A) creates a cause of action for one whose likeness is used by another in a way that is "likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such

---

1.   Deepfakes did in fact appear during the 2020 U.S. election. Fortunately, they were generally either perceptibly fake, identified as fake, or otherwise had a relatively undetectable impact on the outcome of the election. *See* Tom Simonite, *What Happened to the Deepfake Threat to the Election?*, WIRED (Nov. 16, 2020), https://www.wired.com/story/what-happened-deepfake-threat-election/ [https://perma.cc/LVG9-RUPR].

2.   This Note uses the term "deepfake" broadly to refer to digitally manipulated videos, whether they are low-quality or high-quality.

3.   *Synthetic and Manipulated Media Policy*, TWITTER, https://help.twitter.com/en/rules-and-policies/manipulated-media [https://perma.cc/ZKS9-MRC5].

4.   *See* 47 U.S.C. § 230(e)(2). This Note uses the terms "false association" and "false endorsement" interchangeably. Although courts often refer to the claim as "false endorsement," the term "endorsement" does not appear in Section 43(a) of the Lanham Act; Section 43(a) does, however, use the term "association." *See* 15 U.S.C § 1125(a)(1)(A). Section 1125(a) of the Lanham Act is popularly known as Section 43(a). 1 CHARLES E. MCKENNEY & GEORGE F. LONG III, FEDERAL UNFAIR COMPETITION: LANHAM ACT 43A § 1:1 (2021).

person with another person."[5] This Note argues the hypothetical presidential candidate described above, or a similarly harmed individual, can sue the creator of a confusing deepfake using a theory of false association under Section 43(a)(1)(A). Additionally, and crucially, because the individual who posted the deepfake may be unidentifiable and therefore incapable of providing relief, this Note argues a plaintiff could pursue a claim of contributory false association against the owner of a website hosting confusing deepfakes. Unlike defamation claims, which are barred by Section 230 of the Communications Decency Act, injured parties may bring false association claims not only against direct actors, but also against intermediary website operators who knowingly host the misleading content.[6]

This Note begins in Part I by explaining deepfakes and categorizing them based on how the Lanham Act can address them. Next, in Part II, this Note discusses the law of false association under Section 43(a) of the Lanham Act and why it is better suited than alternative legal strategies for addressing deepfakes. Finally, in Part III, this Note discusses the mechanics of a false association claim involving a deepfake, focusing on the issues most likely to present a hurdle to such a claim.

I. DEEPFAKES AND THEIR DANGERS

While certain deepfakes pose harm to society, not all do. Accordingly, the law should distinguish the good from the bad, balancing enforcement with protecting free expression. After explaining how deepfakes are created and distributed in Part I.A., this Note will provide a taxonomy of deepfakes in Part I.B, distinguishing between (i) confusing and, therefore, harmful deepfakes the Lanham Act should address, (ii) non-confusing but harmful deepfakes the Lanham Act cannot address, and (iii) non-harmful deepfakes the Lanham Act should not address. Afterwards, in Part I.C., this Note will discuss potential non-legal solutions to confusing and pernicious deepfakes, before turning to legal solutions in Part II.

---

5. *See* 15 U.S.C § 1125(a)(1)(A).

6. *See* 47 U.S.C. § 230(e)(2); Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001) (holding that the Communications Decency Act does not immunize website owners from trademark infringement claims, because they are intellectual property claims explicitly excluded from the act under Section 230(e)(2)).

A. DEEPFAKES 101

Deepfakes are often created using Generative Adversarial Networks (GANs), which combine generative and discriminative algorithms.[7] Generative algorithms create data based on certain inputs, while discriminative algorithms classify data based on certain inputs.[8] In the case of GANs, both generative and discriminative algorithms take as their inputs large datasets of images, sounds, or videos and work together to create a new image, sound, or video, which approximates those in the dataset but which is not a direct copy of them.[9] The generative algorithm creates new samples, which are then tested by the discriminative algorithm to see if they appear "real" given the input data.[10] As GANs become more sophisticated or use larger data sets as inputs, deepfakes will appear more and more realistic.[11] Since the quality of a deepfake depends on the amount of source material available, individuals whose images and voices are widely available to the public are more susceptible to being imitated via deepfakes.[12]

Due to the ease of sharing content on social media, deepfakes and the information (or misinformation) they convey can spread swiftly. Consider the example of a distorted video, posted in 2019, of Speaker of the House, Nancy Pelosi, which made her speech sound slurred. The video, originally posted on the Facebook page "Politics WatchDog," was shared 45,000 times and viewed over two million times within just one day of its original posting and Rudolph Giuliani's inclusion of it in a Tweet.[13]

---

7.   Mika Westerlund, *The Emergence of Deepfake Technology: A Review*, 9 TECH. INNOVATION MGMT. REV. 39, 40–41 (2019).

8.   Russell Spivak, *"Deepfakes": The Newest Way to Commit One of the Oldest Crimes*, 3 GEO. L. TECH. REV. 339, 342–43 (2019).

9.   *See* Westerlund, *supra* note 7, at 41.

10.   *Id.   See also* Chris Nicholson, PATHMIND, *A Beginner's Guide to Generative Adversarial Networks (GANs)*, A.I. WIKI, https://wiki.pathmind.com/generative-adversarial-network-gan [https://perma.cc/29E5-SRCK] ("One neural network, called the *generator*, generates new data instances, while the other, the *discriminator*, evaluates them for authenticity[.]").

11.   *See* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1760 (2019).

12.   *See* Westerlund, *supra* note 7, at 43.

13.   Drew Harwell, *Faked Pelosi Videos, Slowed to Make Her Appear Drunk, Spread Across Social Media*, WASH. POST. (May 24, 2019), https://www.washingtonpost.com /technology/2019/05/23/faked-pelosi-videos-slowed-make-her-appear-drunk-spread-across-social-media/ [https://perma.cc/UG5D-RRKQ].

Those creating deepfakes may be individuals or foreign governments with political agendas,[14] businesses promoting their products by using others' likenesses, the hosts of YouTube channels or Facebook pages seeking to generate viewership, or trolls—online provocateurs without a particular agenda—taking satisfaction in deceiving the public.[15] Importantly, those initially posting deepfakes to social media are often careful to ensure their anonymity by veiling their IP addresses.[16] As will be discussed in Part II, the anonymity and extra-territoriality of deepfake uploaders can present hurdles to lawsuits against them.

B. A TAXONOMY OF DEEPFAKES

This Note contemplates three categories of deepfakes: (i) deepfakes that are harmful due to their ability to confuse viewers, (ii) deepfakes that are not confusing but are harmful to individuals' dignity and privacy, and (iii) deepfakes that are non-harmful or even socially productive. These three categories, which may at times overlap, are expounded in turn below.[17]

1. *Confusing Deepfakes*

As the Speaker Pelosi example indicates, even low-quality deepfakes can confuse viewers and distort their perceptions of reality. In one of the first known instances of a political party employing deepfakes, Belgium's "sp.a" party released a deepfake of President Donald Trump mocking the Belgian government for

---

14. Researchers from Purdue and Princeton University, for example, have cataloged the growing threat of misinformation campaigns by foreign governments, noting seventy-six influence campaigns between 2013 and 2019. DIEGO A. MARTIN ET AL., EMPIRICAL STUD. OF CONFLICT PROJECT, TRENDS IN ONLINE INFLUENCE EFFORTS 1 (2020), https://esoc.princeton.edu/publications/trends-online-influence-efforts [https://perma.cc/KMD9-LNVU].

15. *See* Westerlund, *supra* note 7, at 41–42.

16. *See* Chesney & Citron, *supra* note 11, at 1792.

17. These categories set the basic parameters for this Note's assessment of legal remedies with respect to deepfakes, which are discussed in Part II and Part III. As will be discussed in Part II, the Lanham Act can be used to hold accountable the creators of and website hosts of confusing deepfakes, i.e., those falling in category (i). Correspondingly, Lanham Act caselaw addressing First Amendment defenses can be used to ensure the creators of socially productive—i.e., category (iii)—deepfakes are protected from false association claims, as discussed in Part III. However, the Lanham Act cannot be applied to deepfakes that do not confuse their viewers. As will be explained in Part II, the intentional infliction of emotional distress tort and the right of publicity are likely best suited for category (ii) deepfakes that harm not by confusion but by insult to dignity.

staying in the Paris climate agreement.[18] The purported intent of the deepfake was to motivate domestic political action on climate change, and sp.a stated, "It is clear from the lip movements that this is not a genuine speech by Trump."[19] Many viewers in Belgium, however, thought the video was real and expressed outrage at the idea of an American president interfering with Belgian policy.[20]

Deepfakes have also emerged in the United States as a means for pursuing political goals. Professors Bobby Chesney and Danielle Citron, for example, have documented a viral deepfake used to undermine the gun control movement.[21] In the aftermath of the February 2018 school shooting in Parkland, Florida, students who survived became national voices in the gun-control movement.[22] One such national voice is Emma González, who was featured in a gun-control advocacy video, in which she rips a piece of paper featuring a bulls-eye target.[23] Soon after the video was released, someone created a deepfake showing González ripping not a bulls-eye but a copy of the United States Constitution.[24] Fortunately, the harm of the video was mitigated by the availability of an original clip of González tearing the bulls-eye, the fact that the video was poorly edited, and the intense media scrutiny of events following Parkland.[25] Nonetheless, it is easy to imagine a situation where an original video is unavailable, the deepfake is higher quality, or media scrutiny comes too late to rectify the harm.

Incidents like these forebode even more perilous uses of deepfakes. On the evening before an election, rival political parties, foreign state actors, or internet trolls could post deepfakes of presidential candidates engaging in lewd acts or criticizing

---

18.   *See* Oscar Schwartz, *You Thought Fake News Was Bad? Deep Fakes Are Where Truth Goes to Die*, GUARDIAN (Nov. 12, 2018), https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth [https://perma.cc/Z8SB-FF2W]; Westerlund, *supra* note 7, at 43. The party's name, "sp.a," was later changed to "Vooruit." Socialist party SP.A to change name to Vooruit, THE BULLETIN (Sep. 15, 2020), https://www.thebulletin.be/socialist-party-spa-change-name-vooruit [https://perma.cc/PF27-PC7F].

19.   Schwartz, *supra* note 18.

20.   *Id.*

21.   *See* Chesney & Citron, *supra* 11, at 1755–57.

22.   *Id.* at 1755.

23.   *Id.* at 1755–56.

24.   *Id.* at 1756.

25.   *Id.*

voters in a swing state.[26] Indeed, Untied States government agencies and intelligence organizations have expressed concern over how deepfakes could be used to undermine national security.[27]

Numerous other risks posed by deepfakes have been extensively documented by other scholars. For example, criminals can create deepfakes for the purposes of blackmail, or terrorist organizations can disseminate deepfakes depicting violence against them in order to garner support.[28] Rogue investors can unleash deepfakes in order to manipulate markets.[29]

The common ground of all of these examples is confusion—due to how realistic the video looks, the unapprised viewer believes the deepfaked individual is engaging in or endorsing the fake actions or statements that are depicted.

2. *Non-Confusing but Harmful Deepfakes*

Although this Note focuses on deepfakes that cause harm by way of confusing their viewers, deepfakes can be harmful even without generating confusion. A common example is pornographic deepfakes. Pornographers (and even amateur video editors) have created deepfakes depicting celebrities engaging in sex acts, and software programs allow users to automatically swap others' faces into sex videos.[30] Social media sites like Reddit and porn sites like Pornhub have banned deepfake sex videos;[31] other sites like

---

26. Nina I. Brown, *Deepfakes and the Weaponization of Disinformation*, 23 VA. J.L. & TECH. 1, 9 (2020) ("A deepfake could be used to provoke mass panic, by depicting the President informing citizens of an imminent or ongoing attack on the U.S. A deepfake could be used to discredit the Supreme Court, by depicting one of the Justices admitting to having taken bribes.").

27. *See* KELLEY M. SAYLER & LAURIE A. HARRIS, CONG. RSCH. SERV., IF11333, DEEP FAKES AND NATIONAL SECURITY (2021); James Rundle, *FBI Warns Deepfakes Might Become Indistinguishable From Reality*, WALL ST. J. (Jan. 17, 2020), https://www.wsj.com /articles/fbi-warns-deepfakes-might-become-indistinguishable-from-reality-11579257004 [https://perma.cc/7K5H-VLHX].

28. *See* Westerlund, *supra* note 7, at 39; Chesney & Citron, *supra* note 11, at 1772 ("Blackmailers might use deep fakes to extract something of value from people, even those who might normally have little or nothing to fear in this regard, who (quite reasonably) doubt their ability to debunk the fakes persuasively, or who fear that any debunking would fail to reach far and fast enough to prevent or undo the initial damage.").

29. Jon Bateman, *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios* 15–17 (Carnegie Endowment for Int'l Peace, Cybersecurity and the Financial System Working Paper No. 7, 2020), https://carnegieendowment.org/files/ Bateman_FinCyber_Deepfakes_final.pdf [https://perma.cc/98EP-QX6K].

30. Chesney & Citron, *supra* note 11, at 1763.

31. Westerlund, *supra* note 7, at 44.

"MrDeepFakes," however, have emerged to cater to those interested in deepfake porn.[32] MrDeepFakes, for example, has a forum, with thousands of comments and hundreds of thousands of views, about how to make pornographic deepfakes, and it even has a forum for requesting such deepfakes to be made.[33] Viewers of videos on sites like MrDeepFakes almost certainly know they are fake; nonetheless, these deepfakes are humiliating to those they target.[34]

3. *Non-Harmful Deepfakes*

Deepfakes are often used in non-confusing ways for improving communication, the arts, and entertainment. The fakery may either be disclosed or obviously understood from the context of the video or the context in which the technology is being used. For example, the Salvador Dalí museum in St. Petersburg, Florida used deepfake technology to bring Dalí "back to life" for educational purposes.[35] Similarly, filmmakers received permission to use Carrie Fisher's and Peter Cushing's personas to create deepfaked versions of Princess Leia and Governor Tarkin, respectively, in *Rogue One: A Star Wars Story*.[36]

While deepfake technology is most often used in the arts and entertainment, it also has been used to alter facial expressions in order to match translated speech or to help people with Alzheimer's recognize their loved ones by making their faces

---

32.   *See* JOHANNES TAMMEKÄND ET AL., SENTINEL, DEEPFAKES 2020: THE TIPPING POINT 82 (2020), https://thesentinel.ai/media/Deepfakes%202020:%20The%20Tipping%20Point,%20Sentinel.pdf [https://perma.cc/YAU9-9UUR].

33.   *Forum Requests*, MRDEEPFAKES (2021), https://mrdeepfakes.com/forums/forum-requests [https://perma.cc/GH6U-45NY] (Stipulating only three limits to the types of deepfakes that can be requested: "1) All requests should be of celebrities only. 2) Celebrities all have to be 18+ of age, preferably over 21. 3) You need 3+ posts to create a request.").

34.   As will be further discussed in Part II, torts such as intentional infliction of emotional distress or the right of publicity are likely best equipped for these situations, where there is harm to dignity but no confusion. This Note, however, focuses on those deepfakes, detailed in the paragraphs above, where the harm stems from viewer confusion.

35.   *Dalí Lives (via Artificial Intelligence)*, SALVADOR DALÍ MUSEUM, https://thedali.org/exhibit/dali-lives/# [https://perma.cc/4VDA-7L4W] (the technology allowed "visitors to interact with an engaging life-like Salvador Dalí on a series of screens throughout the Museum."). *See also* Chesney & Citron, *supra* note 11, at 1769.

36.   *See* Samit Sarkar, *Rogue One Filmmakers Explain How They Digitally Recreated Two Characters*, POLYGON (Dec. 27, 2016), https://www.polygon.com/2016/12/27/14092060/rogue-one-star-wars-grand-moff-tarkin-princess-leia [https://perma.cc/4KQR-ATB9]. *See also* Chesney & Citron, *supra* note 11, at 1770.

appear younger.[37]   Synthesia, for example, is a program that allows users to adapt sound and facial movement in videos to match dozens of different languages.[38]   Some scholars, like Ira Kemelmacher-Shlizerman, believe deepfake technology can also be useful for easing bandwidth constraints during video chats: since audio uses far less bandwidth than video, deepfake technologies can reduce bandwidth by turning audio transmissions into lip-synced, realistic-looking video using locally-stored video and image files to re-construct the faces of people with whom one is video-chatting.[39]

   Other uses of deepfakes are parodic, sometimes signposting in their title or through a watermark that the video is not real. A YouTube user, "Ctrl Shift Face," for example, created a deepfake titled, "The Shining starring Jim Carrey : Episode 1 - Concentration [DeepFake]," which depicted scenes from *The Shining* but with Jack Nicholson's face replaced by Jim Carrey's.[40] In addition to the disclosure of fakery in the title, the description under the video says "it's a deepfake."[41]   Other parodic examples are even more obvious from the context.   For example, one deepfake, posted to YouTube by user "TheFakening," depicts Donald Trump giving a speech alongside his spouse, Melania Trump, but with Vladimir Putin's face superimposed over hers.[42] Even if the video's title were not "Melania Trump Deepfake with Vladimir Putin's Face,"[43] the average viewer would likely recognize the video as fake.

---

37.   *See* Westerlund, *supra* note 7, at 41.

38.   *See Synthesia STUDIO Features*, SYNTHESIA, https://www.synthesia.io/features [https://perma.cc/RM2A-XBVL]; Malaria Must Die, *David Beckham Speaks Nine Languages to Launch Malaria Must Die Voice Petition*, YOUTUBE (Apr. 9, 2019), https://www.youtube.com/watch?v=QiiSAvKJIHo   [https://perma.cc/K42U-72K3]   (a YouTube video using deepfake technology to depict David Beckham speaking in nine different languages to advocate for Malaria Must Die).

39.   *See* Adrienne LaFrance, *The Technology That Will Make It Impossible for You to Believe What You See*, ATLANTIC (July 11, 2017), https://www.theatlantic.com /technology/archive/2017/07/what-do-you-do-when-you-cannot-believe-your-own-eyes/ 533154/ [https://perma.cc/C9TD-877V].

40.   *See* Ctrl Shift Face, *The Shining starring Jim Carrey : Episode 1 - Concentration [DeepFake]*, YOUTUBE (July, 8, 2019), https://www.youtube.com/watch?v=HG_NZpkttXE [https://perma.cc/E53K-TKAC].

41.   *Id.*

42.   TheFakening, *Melania Trump Deepfake with Vladimir Putin's Face*, YOUTUBE (Mar. 11, 2019), https://www.youtube.com/watch?v=K3kgBStHFHs&list=PLWfNGHKv4 EwH64nYpSxT8qh5JnWGj8ymO&index=1 [https://perma.cc/K9M5-35E7].

43.   *Id.*

Deepfakes intended to be parodic may, however, toe the line between obvious parody and confusion as to association, even if they are not intended to deceive their viewers. Advertisers, for example, have used deepfakes, sometimes evocatively, to re-depict famous actors or news anchors in their younger years.[44] State Farm and ESPN, for example, aired a commercial featuring SportsCenter anchor Kenny Mayne digitally manipulated to appear younger.[45] The ad promoted ESPN's documentary series, "The Last Dance," with Kenny Mayne reporting on the Chicago Bull's 1998 NBA championship:

> "This is the kind of stuff that ESPN will eventually make a documentary about," Mr. Mayne says. "They'll call it something like 'The Last Dance.' They'll make it a 10-part series and release it in the year 2020. It's going to be lit. You don't even know what that means yet." As a vintage State Farm logo appears in the background, he adds, "And this clip will be used to promote the documentary in a State Farm commercial."[46]

The creators said, "We tried to make the joke clear enough so that we weren't tricking anyone."[47] Depending on one's media literacy or experience watching SportsCenter, the advertisement may or may not have been confusing.[48]

Likewise, Space150, a creative agency, made a knock-off Travis Scott music video by "feeding the rapper's lyrics into a text generator model, and creating beats and melodies with other neural network programs."[49] The result, called "Jack Park Canny Dope Man" by "Travis Bott," is a "pretty on-brand sound (including the rapper's autotuned voice), although the lyrics are pretty much

---

44.   *See* Tiffany Hsu, *An ESPN Commercial Hints at Advertising's Deepfake Future*, N.Y. TIMES (Apr. 22, 2020), https://www.nytimes.com/2020/04/22/business/media/espn-kenny-mayne-state-farm-commercial.html [https://perma.cc/3FSX-M36P].

45.   *Id.*

46.   *Id.*

47.   *Id.*

48.   Media reports on the commercial indicate some viewers were initially confused by it. Charles Curtis, *A Prescient State Farm Ad with Kenny Mayne Had Everyone Fooled During 'The Last Dance'*, USA TODAY (Apr. 20, 2017), https://ftw.usatoday.com/2020/04/the-last-dance-espn-kenny-mayne-state-farm-ad [https://perma.cc/J7QR-XZRU].

49.   Thom Waite, *Listen to an AI-generated 'Travis Scott' song*, DAZED (Feb. 14, 2020), https://www.dazeddigital.com/music/article/47949/1/listen-to-an-ai-generated-travis-scott-song-artificial-intelligence-deepfake [https://perma.cc/LP5G-MCGU].

completely nonsensical."[50] The video includes footage of a performer appearing to be Travis Scott, and, notably, the YouTube version of the music video does not disclaim a relationship with Travis Scott or disclose that the video is a deepfake.[51] Hence, to uninformed viewers, the music video may seem to be endorsed by the hip-hop artist himself, who was not involved in the project.[52] The takeaway from this and the Kenny Mayne deepfake is that deciding whether a video is harmful by way of confusion as to association may require significant factual investigation.[53]

Considering, though, that the examples discussed above are arguably beneficial to society because their expressive value seems to outweigh the limited, if any, harm by way of viewer confusion, the legal mechanism applied to deepfakes should be able to distinguish harmful from non-harmful uses.[54]

C. NON-LEGAL SOLUTIONS TO HARMFUL DEEPFAKES

Technology companies and government authorities have sought to create deepfake detection tools to combat their deleterious effects caused by confusion. These tools can operate by identifying minor inconsistences such as abnormal reflections, face wobbling, and unnatural mouth movements.[55] They can also be tailored to individuals such as celebrities and politicians who are at a heightened risk of being deepfaked.[56] Microsoft, for example, has released a Video Authenticator Tool, which analyzes subtle blending boundaries and shading "to provide a percentage chance, or confidence score, that the media is artificially manipulated."[57]

---

50. *Id.*
51. *See* Travis Bott, *Travis Bott - JACK PARK CANNY DOPE MAN*, YOUTUBE (Feb. 13, 2020), https://www.youtube.com/watch?v=3UwLhqcZqxc [https://perma.cc/7TNY-MPH8].
52. Davis Gianatasio, *This Agency Used A.I. to Make Travis Bott, a Bogus Travis Scott*, MUSE BY CLIO (Feb. 12, 2020), https://musebycl.io/digital-data/agency-used-ai-make-travis-bott-bogus-travis-scott [https://perma.cc/7GJD-73J9].
53. *See infra* Part II.
54. *See* Brown, *supra* note 26, at 34 ("Banning deepfakes altogether would not only stifle these positive uses but would also raise insurmountable First Amendment hurdles."). As discussed in Part III, trademark law has a well-developed likelihood of confusion doctrine and First Amendment defense, which courts can apply to ensure socially beneficial uses, such as parody, are not stifled.
55. *See* Westerlund, *supra* note 7, at 45.
56. *See id.* at 46.
57. Tom Burt & Eric Horvitz, *New Steps to Combat Disinformation*, MICROSOFT ON THE ISSUES (Sept. 1, 2020), https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/ [https://perma.cc/9ALN-NAPS].

Likewise, malware and cybersecurity companies have developed their own deepfake detection tools—Zemana, a cybersecurity company, created a free program called Deepware, which scans user-uploaded hyperlinks for deepfakes.[58] Despite the availability of these tools, they are not foolproof—researchers have demonstrated the ways such detectors can be tricked.[59]

In light of the opportunity for improvement in deepfake detection technology, some companies have sponsored competitions to encourage innovation. Facebook, for example, organized a Deepfake Detection Challenge, which drew over 2,000 participants; notably, the winning model had an accuracy rate of just 65%.[60] Other technology companies like Google have also made certain datasets publicly available in order to support development of detection tools.[61] Government organizations too, including the Defense Advanced Research Projects Agency (DARPA) of the U.S. Department of Defense, have launched Media Forensics taskforces to pursue deepfake detection solutions.[62] In 2020 the House of Representatives passed the Identifying Outputs of Generative Adversarial Networks (IOGAN) Act, which would, if enacted into law, direct certain agencies to support research on deepfake detection tools.[63]

---

58. *See* DEEPWARE, https://scanner.deepware.ai/result/1a93e77865279476998be27dd6e0a99d70944f13-1608486470/ [https://perma.cc/CQD5-WKVL].

59. University of California San Diego, *Deepfake Detectors Can be Defeated, Computer Scientists Show for the First Time*, SCIENCEDAILY (Feb. 8, 2021), www.sciencedaily.com/releases/2021/02/210208161927.htm [https://perma.cc/HLN4-QHB3].

60. Cristian C. Ferrer et al., *Deepfake Detection Challenge Results: An Open Initiative to Advance AI*, FACEBOOK AI (June 12, 2020), https://ai.facebook.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/ [https://perma.cc/F34V-CUZU] (Facebook launched the challenge by sharing a dataset of more than 100,000 videos, which participants used as a foundation for developing their detection models.).

61. Nick Dufour & Andrew Gully, *Contributing Data to Deepfake Detection Research*, GOOGLE AI BLOG (Sept. 24, 2019), https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html [https://perma.cc/8U6V-ELJB].

62. Matt Turek, *Media Forensics (MediFor)*, DEF. ADVANCED RSRCH. PROJECTS AGENCY, https://www.darpa.mil/program/media-forensics [https://perma.cc/HR3K-L6JF].

63. IOGAN Act, Pub. L. No. 116-258 (2020) (directing the National Science Foundation and the National Institute of Standards and Technology to support research on generative adversarial networks). U.S. legislators have sponsored other bills, which have not passed, calling for the Department of Homeland Security to research and develop deepfake detection tools. *See* DEEP FAKES Accountability Act, H.R. 3230, 116th Cong. (as referred to H. Subcomm. Terrorism & Homeland Sec., June 28, 2019). *See also* Deepfake Report Act of 2019, S. 2065, 116th Cong. (as referred to H. Subcomm. Consumer Prot. & Com., October 29, 2019); Deepfake Task Force Act, S. 2559, 117th Cong. (as referred to S. Comm. on Homeland Sec. and Gov. Affairs).

In addition to efforts to create deepfake detection tools, websites like Twitter have asserted the right to flag or remove videos that "deceptively promote synthetic or manipulated media that are likely to cause harm."[64] As another solution, some scholars have discussed the idea of an "immutable life log or authentication trails that make it possible for a victim of a deep fake to produce a certified alibi credibly proving that he or she did not do or say the thing depicted."[65] Others have proposed digital-watermark solutions that verify the authenticity of video recordings contemporaneously with their production—Canon, for example, has released an "Original Data Security Kit" for verifying the originality of videos made using its products.[66]

Despite these efforts, technologists and legal scholars remain concerned that deepfake creators will continue to outsmart current and emerging detection tools.[67] Hany Farid, a computer scientist at the University of California at Berkeley, has expressed concern that those working on detection are "out-gunned" 100 to 1 by those creating deepfakes.[68] Additionally, even if effective detection tools are developed, it may be difficult to spread awareness about the deepfake, or it may be too late—the harm caused by the deepfake may have already taken place.[69] Moreover, some scholars have

---

64. HELP CENTER, *Synthetic and Manipulated Media Policy*, TWITTER, https://help.twitter.com/en/rules-and-policies/manipulated-media [https://perma.cc/49DN-W2SL]. *See also* Monika Bickert, *Enforcing Against Manipulated Media*, FACEBOOK (Jan. 6, 2020), https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/ [https://perma.cc/J4XD-74Z5].

65. *See, e.g.*, Chesney & Citron, *supra* note 11, at 1814–17. Professors Chesney and Citron note, however, that such a solution's costs to individual privacy may outweigh its potential benefits. *Id.* at 1815–17.

66. *See* Spivak, *supra* note 8, at 353–54 (but noting that such technologies have been hacked and "rendered useless").

67. *See* Brown, *supra* note 26, at 25. *See also* James Vincent, *Deepfake Detection Algorithms Will Never Be Enough*, THE VERGE (June 27, 2019), https://www.theverge.com/2019/6/27/18715235/deepfake-detection-ai-algorithms-accuracy-will-they-ever-work [https://perma.cc/DV47-5Z5S] (warning that detectors will not be able to keep up with technological advancements allowing for increasingly realistic deepfakes).

68. Drew Harwell, *Top AI Researchers Race to Detect 'Deepfake' Videos: 'We are Outgunned'*, WASH. POST (June 12, 2019), https://www.washingtonpost.com /technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/ [https://perma.cc/MJ93-FT9Z].

69. Even if social media companies have access to deepfake detection tools, it may be difficult for them to decide when to remove deepfakes from their sites. Although some deepfakes may be obviously fake or otherwise harmless, the detection tool may not be able to distinguish these from more pernicious deepfakes. *See* Brown, *supra* note 26, at 31. Further, there is the concern that the algorithms of social media sites may spread disinformation faster and wider than the truth. *Id.* at 36 (citing Jared Schroeder,

noted the public may not trust detection tools, even those that are effective.[70] Public distrust in social media companies, for example, may impede acceptance and adoption of such companies' deepfake detection tools.[71]

Even if detection tools become effective at removing harmful deepfakes from public view, such tools fail to disincentivize the creation of harmful deepfakes ex ante. For these reasons, the only resort for victims of deepfakes may be ex post, through the courts, whose adversarial system and power to sanction may provide the trustworthiness and disincentivizing power needed combat pernicious deepfakes.

II. LEGAL STRATEGIES FOR ADDRESSING DEEPFAKES

As deepfakes have both pernicious and non-pernicious uses, as discussed above, any legal approach must be narrowly tailored and not sweep so broadly as to stifle productive speech. Indeed, a wholesale ban on deepfakes would violate the First Amendment.[72]

This Note argues Section 43(a) of the Lanham Act is well-suited for the task of addressing deepfakes due to its focus on consumer confusion, its well-established First Amendment protections, and the fact the Communications Decency Act does not prohibit false association claims against website owners. To be clear, this Note does not purport to argue the Lanham Act is the only appropriate, or necessarily the best, legal mechanism for combatting pernicious deepfakes in all circumstances. Rather, it provides reasons why the Lanham Act is well-suited for the task of taking on deepfake creators and website owners hosting deepfakes, assesses the

---

Marketplace Theory in the Age of AI Communicators, 17 FIRST AMEND. L. REV. 22, 30 (2018)).

70.   Brown, *supra* note 26, at 26 (noting an individual's level of confidence in the deepfake detection software may depend on factors such as ideological views, political biases, and the subject matter of the deepfake, among others).

71.   A 2019 poll by Pew Research Center indicated a substantial portion of the American public distrusted social media sites, with 59% of those surveyed distrusting Facebook. *See* Mark Jurkowitz & Amy Mitchell, *An Oasis of Bipartisanship: Republicans and Democrats Distrust Social Media sites for Political and Election News*, PEW RSCH. CTR. (Jan. 29, 2020), https://www.journalism.org/2020/01/29/an-oasis-of-bipartisanship-republicans-and-democrats-distrust-social-media-sites-for-political-and-election-news/ [https://perma.cc/BS92-H6QT] ("[B]oth Democrats and Republicans (including independents who lean toward either party)—in an unusual display of bipartisan convergence—register far more distrust than trust of social media sites as sources for political and election news. And the most distrusted are three giants of the social media landscape—Facebook, Instagram and Twitter.").

72.   *See* Spivak, *supra* note 8, at 399.

merits of other legal strategies that have been proposed, and, in Part III, articulates the mechanics of Lanham Act false association claim, which need not be the exclusive cause of action in a deepfake-related suit.

A. SECTION 43(a)(1)(A) OF THE LANHAM ACT

The false association claim contemplated by this Note is premised on the theory that the target of a confusing deepfake— i.e., the video's human subject, who has an intellectual property right in the use of her persona—is falsely portrayed to be associated with or otherwise endorsing the message or actions depicted in the video. The false association cause of action is codified in Section 43(a)(1)(A) of the Lanham Act, the United States trademark and false advertising statute.[73]

A principal goal of trademark law and the Lanham Act is consumer protection—i.e., protecting the public from deception.[74] The text of the Act, its construction by the federal courts, and congressional statements concurrent to the Act's passage confirm consumer protection as a goal of trademark and unfair competition law.[75] While, historically, the Act focused primarily on fostering competition and preventing deceptive uses of marks by competitors, it has gradually expanded to prohibit even noncompetitive uses of a mark likely to deceive consumers as to association or endorsement.[76]

Section 43(a)(1)(A) of the Lanham Act, in particular, was initially intended to prohibit false designations of geographic origin, such as Canadian perfume advertised as "Parfum de

---

73.   *See* 15 U.S.C. § 1125(a)(1)(A)–(B).

74.   *See, e.g.*, 1 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 2:22 (5th ed. 2020) ("Trademark protection is consumer protection"); *id.* at § 2:24 (quoting Guthrie Healthcare System v. ContextMedia, Inc., 826 F.3d 27, 50 (2d Cir. 2016) ("An important beneficiary of the trademark system is the public.")); *id.* at § 2:1 (tracing the historical origins of trademark and unfair competition law to Anglo-American Courts of Chancery and Courts of Law, and noting the case law of the latter focused on protecting against "fraud and deceit practiced by the defendant on the public").

75.   *See id.*

76.   MCCARTHY, *supra* note 74, at § 5:2 ("The growth of trademark protection from only competitive parties to include noncompetitive uses of a mark, signaled a large expansion in the protection of marks. This expansion gradually continued in fits and starts until by the late twentieth century, it was very clear that a strong mark could be protected against use on noncompetitive goods or services so long as there was a likelihood of confusion over sponsorship, affiliation or connection.").

France."[77]   Over time, however, courts interpreted Section 43(a)(1)(A) more broadly to prohibit false designations of source, sponsorship, and other forms of unfair competition.[78] This more capacious understanding was codified when Congress amended Section 43(a) in 1988.[79]   Since then, courts have continued to broadly interpret Section 43(a)(1)(A) as covering a wide range of rights, including that of an individual to the use of her likeness as an endorsement.[80] The text of Section 43 that is most relevant to this Note is reproduced below:

> (a) Civil action
>   (1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—
>   (A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or
>   (B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.[81]

Notably, Section 43(a) does not require registration as a prerequisite for suit, and it has "been held to apply to situations that would not qualify formally as trademark infringement, but that

---

77.   JANE C. GINSBURG ET AL., TRADEMARK AND UNFAIR COMPETITION LAW: CASES AND Materials 478 (6th ed. 2017).
78.   *Id.*
79.   *Id.*
80.   *Id. See also* MCCARTHY, *supra* note 74, at § 28:15 (5th ed. 2020) ("[T]he 1989 revised wording of § 43(a) makes it clearer than ever that § 43(a) is an appropriate vehicle for the assertion of claims of falsely implying the endorsement of a product or service by a real person.").
81.   15 U.S.C. § 1125(a)(1)(A)–(B).

involve unfair competitive practices resulting in actual or potential deception."[82]

Courts have read Section 43(a)(1)(A), specifically, to prohibit the unauthorized use of an individual's persona—as manifest in a video or photograph,[83] an audio-recording of one's voice,[84] or even, in some cases, a look-alike robot[85]—that "creates the false impression that the party has endorsed a product or service in interstate commerce."[86] Plaintiffs need not show that consumers are likely to "believe that the owner of the mark actually produced the item and placed it on the market."[87] Instead, it is sufficient to show the public is likely to believe the "mark's owner *sponsored or otherwise approved*" the use of the plaintiff's image.[88]

At issue in *Allen v. National Video*, for example, was defendant National Video's advertisement for its video rental chain, which starred a Woody Allen look-alike, Phil Boroff, "smiling at the camera while holding up [National Video's] V.I.P. card."[89] Although the look-alike did not explicitly endorse the video rental chain, the U.S. District Court for the Southern District of New York granted summary judgment for plaintiff Woody Allen on his

---

82. Allen v. Nat'l Video, Inc., 610 F. Supp. 612, 625 (S.D.N.Y. 1985) (citing SK & F, Co. v. Premo Pharm. Lab'ys, Inc., 625 F.2d 1055, 1065 (3d Cir.1980)). *See also* Cher v. F. Int'l, Ltd., No. 81 1461 R., 1982 WL 916836, at *6 (C.D. Cal. Jan. 15, 1982) (registration of an actual trademark is not required for suit under Section 43). *See infra* Part III.A, discussing the issue of standing.

83. *See, e.g.*, Downing v. Abercrombie & Fitch, 265 F.3d 994, 1008–09 (9th Cir. 2001) (reversing summary judgment for defendant on question of false endorsement, where defendant Abercrombie used professional surfers' photos without their permission in a catalog: "A jury could reasonably find that Abercrombie intended to indicate to consumers that these legendary surfers were endorsing Abercrombie's merchandise."); Fifty-Six Hope Road Music, Ltd. v. A.V.E.L.A., Inc., 778 F.3d 1059, 1067 (9th Cir. 2015) (affirming jury verdict of false endorsement, where the defendant used an unauthorized image of Bob Marley on its T-shirts).

84. *See, e.g.*, Waits v. Frito-Lay, Inc. 978 F.2d 1093, 1111 (9th Cir. 1992) (affirming jury verdict of false endorsement, where defendant Frito-Lay used a voice-impersonator of plaintiff Tom Waits in its Doritos commercial, which likely caused ordinary consumers to be "confused as to whether Tim Waits sang on the commercial").

85. *See* White v. Samsung Elecs. Am., Inc., 971 F.2d 1395, 1396 (9th Cir. 1992); Wendt v. Host Int'l, Inc., 125 F.3d 806 (9th Cir. 1997).

86. *Allen*, 610 F. Supp. at 626. *See also* MCCARTHY, *supra* note 74, at § 28:15 (noting that 43(a)(1)(A) does not require the plaintiff to establish the "traditional indicia" of a trademark right).

87. Famous Horse Inc. v. 5th Ave. Photo Inc., 624 F.3d 106, 109 (2d Cir. 2010) (quoting Dallas Cowboys Cheerleaders, Inc. v. Pussycat Cinema, Ltd., 604 F.2d 200, 204 (2d Cir. 1979)).

88. *Id.* (emphasis in original).

89. Allen v. Nat'l Video, Inc., 610 F. Supp. 612, 617, 627 n.8 (S.D.N.Y. 1985), cited by, *e.g.*, Est. of Smith v. Cash Money Recs., Inc., No. 14CV2703, 2018 WL 2224993, at *8 (S.D.N.Y. May 15, 2018).

false endorsement claim.[90] The court noted, "When a public figure of Woody Allen's stature appears in an advertisement, his mere presence is inescapably . . . interpreted as an endorsement."[91] To find false association, the court applied trademark law's traditional likelihood of confusion standard—"'the heart of a successful claim' under both the Lanham Act and common law trademark infringement."[92]

As this Note argued in Part I, harmful deepfakes can generally be differentiated from non-harmful deepfakes based on whether they confuse the viewer—where there is no confusion, there is generally no harm inflicted by the deepfake.[93] Since the "heart of a successful claim" under the Lanham Act is the likelihood of confusion test, Section 43(a) of the Lanham Act and its associated caselaw is equipped to differentiate the good deepfakes from the bad.

Likewise, trademark law's well-developed First Amendment precedent suits it to the task of differentiating between harmful and non-harmful deepfakes. In Lanham Act disputes, courts generally apply the *Rogers* test to balance free speech rights with protection of consumers from deception in trademark cases.[94] The two-part *Rogers* test, discussed further in Part III, upholds expressive use of a mark unless (i) it has "no artistic relevance" to the disputed work or, (ii) if there is artistic relevance, the use "explicitly misleads as to the source or the content of the work."[95] The test significantly limits the reach of the Lanham Act and would serve to protect parodic (and non-pernicious) deepfakes from claims of false association.[96]

A significant benefit of a false association action, discussed further in Part III, is that the Communications Decency Act does not immunize website owners from federal intellectual property

---

90.   *Id.* at 627–28, 629–30. Notably, the court stated that in the future the defendant would be required to either provide a "bold and unequivocal disclaimer" or otherwise "make it completely clear that he *is* a look-alike and that the plaintiff has nothing to do" with his work. *Id.* at 630 (emphasis in original).

91.   *Id.* at 627 n.8.

92.   *Allen*, 610 F. Supp. at 627 (quoting Standard & Poor's Corp. v. Commodity Exch., Inc., 683 F.2d 704, 708 (2d Cir.1982)).

93.   The primary exception to this generalization, discussed *supra* Part I.B.2, is deepfake porn, when viewers know the video is fake but there is nevertheless harm to the target's dignity.

94.   MCCARTHY, *supra* note 74, at § 28:16.

95.   Rogers v. Grimaldi, 875 F.2d 994, 999 (2d Cir. 1989).

96.   *See* Mark A. Lemley, *Privacy, Property, and Publicity*, 117 MICH. L. REV. 1153, 1173 (2019).

claims such as those under Section 43(a)(1)(A) of the Lanham Act.[97]   In fact, Section 230(e)(2) of the CDA explicitly states, "Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property."   A plaintiff would still need to establish the secondary liability of website owners; however, unlike a defamation claim, a false association claim at least is not strictly barred by Section 230.[98]

Despite these potential advantages of a false association claim against deepfake creators, the claim has certain downsides.   As will be discussed in Part III, it may be difficult for non-celebrity plaintiffs to show they have a commercial interest in their likeness, which some courts require to achieve standing under Section 43(a) of the Lanham Act.[99]   Likewise, the courts may have trouble accepting that a defendant's use of a deepfake was "in connection with any goods or services" for the purposes of Section 43(a).[100] Additionally, as discussed above, one could not bring a Lanham Act claim against the creators of deepfakes that are harmful to one's dignity but unlikely to confuse their viewers, such as pornographic deepfakes with visible disclaimers.   Other downsides include the lack of standing for a confused consumer (as opposed to the target of the deepfake) to sue under Lanham Act 43(a),[101] and the potential difficulty of establishing secondary liability against website owners, as discussed further in Part III.

B. TORT LAW

While the Lanham Act offers certain advantages for addressing the issue of deepfakes, other legal strategies are also applicable. In particular, this Part explores the viability of tort law claims, including defamation, intentional infliction of emotional distress, and the privacy torts.

In most jurisdictions, defamation via libel requires a showing of "(1) a written false and defamatory statement of fact concerning the plaintiff; (2) that was published by the defendant to a third party; (3) due to the defendant's negligence or actual malice, depending on the status of the person libeled; and (4) special

---

97.   47 U.S.C. § 230(e)(2).
98.   *Id.*
99.   *See* MCCARTHY, *supra* note 74, at § 28:17.
100.   *See* 15 U.S.C. § 1125.
101.   MCCARTHY, *supra* note 74, at § 27:39.

damages or *per se* actionability."[102]   Considering the near impossibility of creating a deepfake by accident, plaintiffs could generally satisfy the showing of actual malice or reckless disregard as to the potential falsity of the deepfake, which would be required if the deepfake involved a public figure.[103] Defamation law's *per se* categories—statements that impute a criminal offense, loathsome disease, misconduct in business or office, or sexual misconduct— could also benefit plaintiffs, because claims involving deepfakes in these *per se* categories are entitled to general damages, and some pernicious deepfakes tend to invoke at least one of these categories.[104] Hence, the defamation tort can potentially provide civil plaintiffs with robust damages claims.[105]

Because many deepfakes are uploaded anonymously, however, it may be difficult to identify the appropriate defendant, and a plaintiff's only remedy may be against a website owner. Hence, the primary downside to defamation law is that the Communications Decency Act immunizes websites from liability for defamation by third-party posters.[106] In other words, a plaintiff is likely completely foreclosed, under defamation law, from achieving injunctions against third-party websites onto which a deepfake was shared.[107]   A claim of intentional infliction of emotional distress, which requires a showing of "extreme and outrageous conduct"[108] might also be applicable to deepfakes depicting especially offensive actions; however, the CDA similarly would bar such a claim against website owners.[109]

In addition to defamation and intentional infliction of emotional distress, the privacy torts—intrusion upon seclusion, publicity given to private life, false light, and right of publicity (misappropriation)—are relevant to deepfakes, but each has a different potential for success. The intrusion upon seclusion tort

---

102.   Spivak, *supra* note 8, at 370 (quoting Daytree at Cortland Sq., Inc. v. Walsh, No. 15CV2298JFBAYS, 2018 WL 3869247 at *9 (E.D.N.Y. Aug. 15, 2018). *See also* Celle v. Filipino Reporter Enters., 209 F.3d 163, 176 (2d Cir., 2000)., cited by Russell Spivak, "Deepfakes": The Newest Way to Commit One of the Oldest Crimes, 3 GEO. L. TECH. REV. 339, 366 (2019).

103.   Chesney & Citron, *supra* note 11, at 1793. *See also* Spivak, *supra* note 8, at 366 (citing New York Times Co. v. Sullivan, 376 U.S. 254 (1964)).

104.   *See* Spivak, *supra* note 8, at 374–75.

105.   Chesney & Citron, *supra* note 11, at 1795.

106.   47 U.S.C. § 230(c)(1).

107.   *See id.*

108.   *See* Chesney & Citron, *supra* note 11, at 1753.

109.   *See* 47 U.S.C. § 230(c)(1).

is based on the manner by which an intruder acquires information rather than on the falsity of information.[110] As deepfakers generally create videos from publicly available photos or videos of their targets, they are unlikely to be covered by the intrusion upon seclusion tort.[111] Similarly, the public disclosure of private fact tort is generally inapplicable to deepfakes, because one of the tort's "essential" elements is that the facts at issue are actually true;[112] the damaging aspects of most deepfakes—often egregious statements or depictions of violent, sexual, or other activities—are likely to be false and therefore not actionable under the public disclosure of private fact tort. The false light tort and the right of publicity, however, are more applicable to deepfakes. The former is not recognized by many jurisdictions,[113] because it is perceived as substantially overlapping with the defamation tort.[114] The latter, however, has gained traction with the courts and state legislatures, and it is particularly relevant to deepfakes.[115]

Although the right of publicity's origins lie in state privacy law, it has been described as an intellectual property right and is similar to the false association claim proposed by this paper.[116] To establish a claim, the plaintiff usually must show (i) the defendant used an aspect of the plaintiff's identity or persona, without consent, in such a way that the plaintiff is identifiable from the

---

110. Spivak, *supra* note 8, at 379. *See also* RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

111. *See* Spivak, *supra* note 8, at 379.

112. Spivak, *supra* note 8, at 379 (quoting Tyne ex rel. Tyne v. Time Warner Ent. Co., L.P., 204 F. Supp. 2d 1338, 1344 (M.D. Fla. 2002), *aff'd sub nom.* Tyne v. Time Warner Ent. Co., L.P., 425 F.3d 1363 (11th Cir. 2005). *See also, e.g.*, Wood v. Hustler Mag., Inc., 736 F.2d 1084, 1090, 1093 (5th Cir. 1984) (applying Texas law and finding defendant Hustler liable for the false light tort but not the public disclosure of private facts tort, because the information accompanying Hustler's disclosure of plaintiff's photo was not truthful), cited by Spivak, *supra* note 8, at 378.

113. *See, e.g.*, Jews For Jesus, Inc. v. Rapp, 997 So. 2d 1098, 1113 (Fla. 2008).

114. *Id.* ("Based upon our review of the law in Florida and in many other jurisdictions, we simply cannot ignore the significant and substantial overlap between false light and defamation."). *See also* J. Clark Kelso, *False Light Privacy: A Requiem*, 32 SANTA CLARA L. REV. 783, 785 (1992) (reviewing hundreds of false light cases and arguing "there is not even a single good case in which false light can be clearly identified as adding anything distinctive to the law.").

115. *See* Spivak, *supra* note 8, at 383–86.

116. 1 J. THOMAS MCCARTHY & ROGER E. SCHECHTER, RIGHTS OF PUBLICITY AND PRIVACY §§ 1:2, 1:3 (2d ed. 2021) ("The right of publicity is a state-law created intellectual property right whose infringement is a commercial tort of unfair competition."). Courts and commentators have even described Lanham Act false endorsement claims as the "federal equivalent of the right of publicity." *See* ETW Corp. v. Jireh Pub., Inc., 332 F.3d 915, 924 (6th Cir. 2003) (citing Bruce P. Keller, *The Right of Publicity: Past, Present, and Future*, 1207 PLI CORP. LAW AND PRAC. HANDBOOK, 159, 170 (2000)).

defendant's use, and (ii) defendant's use is likely to cause damage to the commercial value of the plaintiff's persona.[117] Most states recognize the right of publicity cause of action either via common law or via statute.[118] New York, for example, has codified the right of publicity, calling it the "Right of Privacy," which creates a private action for injunction and damages for:

> Any person whose name, portrait, picture or voice is used within this state for advertising purposes or for the purposes of trade without the written consent first obtained . . .[119]

As deepfakes appropriate the persona of others for their own purposes, the right of publicity is a particularly relevant cause of action. Although it is similar to the false association cause of action, it differs in one critical way—falsity or likelihood of confusion is not an element of the right of publicity tort.[120] Instead, central to a right of publicity claim is the identifiability of the plaintiff in the allegedly infringing article.[121]

The right of publicity's focus on identifiability, rather than on confusion, can lead to different results than false association claims. In *Allen v. National Video, Inc.*, for example, the court concluded that plaintiff Woody Allen's suit against National Video for its use of a Woody Allen look-alike was "more properly regarded as one for unfair competition [i.e., false association] under the Lanham Act," as opposed to one for the right of publicity.[122] In *Allen*, there was "at least a likelihood of consumer confusion as to whether plaintiff endorse[d] National Video," making the Lanham Act well-suited for the claim.[123] Contrastingly, the fact that the defendant used a look-alike, rather than an image of Woody Allen himself, presented "difficult questions of law and fact" as to whether National Video could be liable under a right of publicity claim, which requires use of the plaintiff's "portrait" or "picture."[124]

---

117.   MCCARTHY & SCHECHTER, *supra* note 116, at § 3:2.

118.   *See id.* at §§ 1:2, 1:36, 6:6.

119.   N.Y. CIV. RIGHTS LAW § 51 (McKinney 2021).

120.   MCCARTHY, *supra* note 74, at § 28:7.

121.   *Id.* at § 28:12.

122.   Allen v. Nat'l Video, Inc., 610 F. Supp. 612, 632 (S.D.N.Y. 1985).

123.   *Id.*

124.   *Id.* at 632, 624 ("The substantive standard of likelihood of confusion provided by the Lanham Act, discussed below, seems more appropriate than the somewhat strained construction required here under section 51. . . . Moreover, the relief available to plaintiff is virtually identical under either theory.").

Hence, the court resolved the matter under the Lanham Act instead of under the New York right of publicity statute, granting summary judgment on the false endorsement claim in favor of Allen.[125] However, in other cases, it may be easier to establish "identifiability" under a right of publicity theory than confusion under a false association theory. As McCarthy has noted:

> All other things being equal, it will often be easier for a plaintiff to prove "identifiability" infringement of the right of publicity than to prove "likelihood of confusion" infringement of a trademark right. A defendant's unpermitted use which does not satisfy the trademark test of "likelihood of confusion" may satisfy the lesser "identifiability" test of the right of publicity. As Judge Nies observed: "There may be no likelihood of such confusion as to the source of goods even under a theory of 'sponsorship' or 'endorsement,' and, nevertheless, one's right of privacy, or the related right of publicity, may be violated."[126]

However, as this Note contends that viewer confusion is the touchstone of most pernicious deepfakes,[127] the Lanham Act's focus on confusion makes the law generally well-suited to ensuring only worthy claims proceed against deepfake creators.

The First Amendment doctrine as applied to false association claims is similarly focused on confusion, unlike in the case of the right of publicity. Two cases decided on the same day by the Ninth Circuit—*Brown v. Electronic Arts, Inc.* and *In re NCAA Student-Athlete Name & Likeness Licensing Litigation*—demonstrate how courts treat First Amendment defenses to false association and to the right of publicity differently.[128] At issue in both cases was EA Sports' use of athletes' likenesses in its football video games. The facts of the cases were essentially identical: in both, EA Sports used the plaintiffs' likenesses—their recognizable facial features, skin tone, hair color, age, height, weight, etc. (but not their actual

---

    125.   *Id.* at 624.
    126.   McCarthy, *supra* note 74, at § 28:12 (quoting Univ. of Notre Dame Du Lac v. J.C. Gourmet Food Imps. Co., 703 F.2d 1372, 1376 (Fed. Cir. 1983)).
    127.   *See supra* Part II.
    128.   Brown v. Elec. Arts, Inc., 724 F.3d 1235 (9th Cir. 2013); In re NCAA Student-Athlete Name & Likeness Licensing Litig., 724 F.3d 1268 (9th Cir. 2013). *See also* Lemley, *supra* note 96, at 1175–77.

names)—without consent in their video games.[129]   There was, however, one critical difference between the cases: in *Brown*, the plaintiff formulated his claim in terms of false association under Section 43(a) of the Lanham Act; whereas, in *NCAA*, the plaintiffs formulated their claims under California's common law and statutory right of publicity.[130]   This difference resulted in the Ninth Circuit rejecting the plaintiff's false association claim using the *Rogers'* First Amendment test in *Brown*, but upholding the plaintiffs' right of publicity claim in *NCAA*, where the court did not apply *Rogers*, reasoning:

> [W]e disagree that the *Rogers* test should be imported wholesale for right-of-publicity claims.   Our conclusion on this point is consistent with the Third Circuit's rejection of EA's identical argument in *Hart*. . . . As the history and development of the *Rogers* test makes clear, it was designed to protect consumers from the risk of consumer confusion— the hallmark element of a Lanham Act claim. . . . The right of publicity, on the other hand, does not primarily seek to prevent consumer confusion.   *See Hart*, 717 F.3d at 158 ("[T]he right of publicity does not implicate the potential for consumer confusion . . . ."). Rather, it primarily "protects a form of intellectual property [in one's person] that society deems to have some social utility." . . . The right of publicity protects the celebrity, not the consumer.   Keller's publicity claim is not founded on an allegation that consumers are being illegally misled into believing that he is endorsing EA or its products.[131]

Courts have at times, and sometimes inconsistently, applied the *Rogers* test to right of publicity claims.[132]   In *NCAA*, the Ninth

---

129.   *See Brown*, 724 F.3d at 1240; *In re NCAA Student-Athlete Name & Likeness Licensing Litig.*, 724 F.3d at 1271.

130.   *See Brown*, 724 F.3d at 1240; *In re NCAA Student-Athlete Name & Likeness Licensing Litig.*, 724 F.3d at 1272.

131.   *In re NCAA Student-Athlete Name & Likeness Licensing Litig.*, 724 F.3d at 1280 (internal citations omitted).   Jennifer Rothman has criticized this difference in First Amendment treatment between the right of publicity and false endorsement, arguing the lack of harmony allows the right of publicity to "thwart the speech protections provided for" in the Lanham Act. JENNIFER ROTHMAN, THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD 158 (2018).

132.   *See id.* at 1281 (discussing the Sixth Circuit's inconsistent application of *Rogers* in right of publicity cases, and the Eighth and Tenth Circuits' rejection of the *Rogers* test in right of publicity cases); MCCARTHY & SCHECHTER, *supra* note 116, at § 8:23 (noting that

Circuit refused to apply *Rogers* and instead applied a five factor transformative use test, which proved less protective of free speech than the *Rogers* test.[133] Considering confusion is deepfakes' principal harm and that there are numerous beneficial uses of deepfakes, the arguably more protective, confusion-focused *Rogers* test,[134] as applied in the context of the Lanham Act, is best suited to filter the unworthy from the worthy claims against deepfake creators.

The most significant drawback to the right of publicity claim is that certain courts do not allow plaintiffs to proceed against website owners for claims of secondary liability. Although the Communications Decency Act provides an exception from immunity for intellectual property claims, and the right of publicity has been construed as an intellectual property right, the Ninth Circuit has ruled that the CDA's exception for intellectual property only extends to federal (i.e., not state) intellectual property claims, hence barring right of publicity claims against website owners on theories of secondary liability.[135] Finally, another disadvantage to the right of publicity tort, as compared to false association, is states' diverse treatment of it. As the right of publicity differs state by state,[136] injunctions may be limited in geographical scope.[137] Because the Lanham Act is federal law,

---

only the Sixth circuit has applied the *Rogers* test in right of publicity cases and stating that the problem with applying the *Rogers* test is it is "a falsity-based test which does not fit with the right of publicity, which has no requirement of falsity.").

133.   *In re NCAA Student-Athlete Name & Likeness Licensing Litig.*, 724 F.3d at 1274.

134.   *Contra* Rogers v. Grimaldi, 875 F.2d 994, 1004 (2d Cir. 1989) ("Because the right of publicity, unlike the Lanham Act, has no likelihood of confusion requirement, it is potentially more expansive than the Lanham Act. Perhaps for that reason, courts delineating the right of publicity, more frequently than in applying the Lanham Act, have recognized the need to limit the right to accommodate First Amendment concerns.") (citations omitted).

135.   Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1119 (9th Cir. 2007) (limiting the CDA's intellectual property exception to immunity for federal intellectual property law claims). *But see* Hepp v. Facebook, 14 F.4th 204, 206 (3d Cir. 2021) (holding that Section 230 does not bar right of publicity claims, because they fall under Section 230(e)(2)'s intellectual property exception). *See also* MCCARTHY & SCHECHTER, *supra* note 116, at § 3:19.

136.   *See* MCCARTHY & SCHECHTER, *supra* note 116, at § 6:6.

137.   *See* Allen v. Nat'l Video, Inc., 610 F. Supp. 612, 630 (S.D.N.Y. 1985) ("Defendants have argued that any injunction against them must be limited in geographical scope to New York State. While such a limitation might be required for an injunction under the New York Civil Rights Law, given the differences in privacy law among different jurisdictions, an injunction under the Lanham Act need not be so limited.").

however, injunctions resulting from false association actions are similarly enforceable across all U.S. jurisdictions.[138]

Despite these disadvantages, the right of publicity has two potential advantages over false association. One such advantage is the right of publicity does not necessarily require the plaintiff to be a public figure with a commercial interest in her identity;[139] whereas, as will be discussed in Part III, some courts require plaintiffs to have a commercial interest in their identity in order to state a false association claim.[140] The other advantage of the right of publicity is it provides a remedy to harms caused by damage to dignity rather than by confusion or falsity. As discussed previously in Part I, viewers may be aware that individuals in pornographic deepfakes did not actually engage in the acts depicted—i.e., such videos may not cause confusion—hence generally precluding liability under the Lanham Act.[141] Nevertheless, the targets of these videos suffer harm to their dignity and privacy, which may be more appropriately addressed by the right of publicity.

C. COPYRIGHT LAW

In addition to the tort-based claims discussed above, commentators have considered copyright, regulatory, criminal, and statutory approaches to deepfakes. Although Section 230 of the Communications Decency Act does not bar contributory copyright infringement claims,[142] copyright law is unlikely to offer substantial relief. As an initial matter, the targets of deepfakes are unlikely to be copyright owners of the images or videos that form the basis of the disputed deepfake.[143] Only the owners of the copyright in the underlying images have standing to sue, and, as Russell Spivak argues, they are unlikely to do so in order to vindicate deepfake victims or the general public, given the

---

138. *Id.*
139. MCCARTHY & SCHECHTER, *supra* note 116, at § 3:13 ("The clear majority view is that a non-celebrity can sue for the unpermitted commercial use of his or her identity.").
140. MCCARTHY, *supra* note 74, at § 28:17.
141. In some cases, courts have glossed over the likelihood of confusion issue in order to find Lanham Act liability due to moralistic concerns. *See* Dallas Cowboys Cheerleaders, Inc. v. Pussycat Cinema, Ltd., 604 F.2d 200, 205 (2d Cir. 1979) ("Indeed, it is hard to believe that anyone who had seen defendants' sexually depraved film could ever thereafter disassociate it from plaintiff's cheerleaders.").
142. *See* 47 U.S.C. § 230(e)(2) (stating that Section 230 does not limit intellectual property laws).
143. *See* Spivak, *supra* 8, at 396–98.

expenses of litigation and the arguably minimal harm they incurred as a result of the infringement.[144] Further, as Professor Nina Brown has argued, even if the photos or videos from which a deepfake is derived are subject to copyright protection, the resulting deepfake is a new creation, which may be upheld under copyright's fair use doctrine.[145] One potential benefit of copyright law is the notice and takedown process of the Digital Millennium Copyright Act (DMCA), which provides a less-costly and potentially more effective alternative to copyright suit. The DMCA incentivizes websites to take down infringing material by providing immunity from infringement suits for doing so in compliance with the act's procedures.[146] However, as Russell Spivak notes, the copyright owner rather than the target of the deepfake would have to initiate the process.[147] Further, the copyright owner would ultimately still need to have a valid copyright claim against the alleged infringer, which, as noted, is uncertain, given copyright's fair use doctrine.[148]

D. REGULATORY SOLUTIONS

Other scholars have addressed the possibility of deepfake regulation by Federal administrative agencies such as the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), or the Federal Election Commission (FEC). Some deepfakes in the context of advertising may naturally fall under the FTC's purview—the regulation of "unfair or deceptive acts or practices in or affecting commerce."[149] However, attempts by the FTC—a government entity—to distinguish between "true" and "false" information and to regulate false information, is likely to raise First Amendment concerns.[150] The FCC may be a better candidate: while the FCC's jurisdictional authority to regulate

---

144.   *See id.*
145.   *See* Brown, *supra* note 26, at 40 n.132; 17 U.S.C.A. § 107 (Westlaw through Pub. L. No. 117-41).
146.   *See* Spivak, *supra* note 8, at 398–99.
147.   *Id.*
148.   *Id.*
149.   Federal Trade Commission Act, 15 U.S.C. § 45(a)(1); Chesney & Citron, *supra* note 11, at 1806. *See also* Elizabeth Caldera, *"Reject the Evidence of Your Eyes and Ears": Deepfakes and the Law of Virtual Replicants*, 50 SETON HALL L. REV. 177, 178 (2019) (discussing possible administrative agency solutions to the issue of deepfakes and ultimately proposing that the FTC is best suited to regulate deepfakes).
150.   Chesney & Citron, *supra* note 11, at 1806.

information circulating over social media is debatable,[151] the agency has asserted its authority to engage in rulemaking on Section 230 of the CDA.[152] Whether and how, specifically, the FCC would regulate social media remains to be seen, however. Professors Chesney and Citron have also discussed the FEC as a possible regulator of deepfakes, noting the potential for it to require deepfake creators to disclose fakery in the context of campaigns.[153] They note, however, that the FEC's jurisdiction over deepfakes is dubious: it does not have clear jurisdiction over the social media platforms on which deepfakes most frequently spread, it does not currently regulate the truth of campaign statements, and, regardless, it does not have jurisdiction outside the context of elections.[154] Moreover, as the targets of deepfakes have the incentive to sue under defamation, privacy tort, or false association causes of action, there is less of a rationale for intervention by government regulators.[155] Most importantly, "the prospect of a government entity attempting to distinguish real news from fake news—and suppressing the latter—raises serious First Amendment concerns."[156] Together, these concerns pose significant hurdles to a regulatory solution for deepfakes.

E. STATE AND FEDERAL STATUTES

Criminal law, too, has been invoked as a method of combatting deepfakes. Texas, for example, was the first state to pass a law criminalizing deepfakes that are made "with intent to influence the outcome of an election.[157] The Texas law reads:

---

151. *Id.* at 1807.
152. Thomas M. Johnson, Jr. *The FCC's Authority to Interpret Section 230 of the Communications Act*, FEDERAL COMMUNICATIONS COMMISSION (Oct. 21, 2020), https://www.fcc.gov/news-events/blog/2020/10/21/fccs-authority-interpret-section-230-communications-act [https://perma.cc/W4PY-B7HW]. *See also* Darrell M. West, *What to Expect from a Biden FCC on Section 230, Net Neutrality, and 5G*, BROOKINGS (Dec. 3, 2020), https://www.brookings.edu/blog/techtank/2020/12/03/what-to-expect-from-a-biden-fcc-on-section-230-net-neutrality-and-5g/ [https://perma.cc/UL7F-K3EZ].
153. Chesney & Citron, *supra* note 11, at 1806.
154. *Id.*
155. *Id.*
156. *Id.*
157. TEX. ELEC. CODE ANN. § 255.004 (West 2019); S.B. 751, 2019 Leg., 86th Sess. (Tex. 2019); Brown, *supra* note 26, at 9 (arguing the law may not survive strict scrutiny under the First Amendment, because it prohibits speech based on whether it is false, which has been rejected by the Supreme Court) (citing United States v. Alvarez, 567 U.S. 709, 718 (2012)).

(d) A person commits an offense if the person, with intent to injure a candidate or influence the result of an election:

    (1) creates a deep fake video; and

    (2) causes the deep fake video to be published or distributed within 30 days of an election.

(e) In this section, "deep fake video" means a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality.[158]

Likewise, Virginia has passed a law criminalizing the distribution of nonconsensual deepfake porn as a Class 1 misdemeanor, punishable by a fine of $2,500 and up to one year in jail.[159] In addition to passing criminal laws, other states such as California have passed laws providing for private causes of action against the creators of deepfakes used for political manipulation and pornography without permission.[160]

Members of U.S. Congress have also proposed legislation combatting deepfakes. Senator Ben Sasse of Nebraska, for example, sponsored the Malicious Deep Fake Prohibition Act of 2018, which would make it a federal felony to create deepfakes intended to "facilitate criminal or tortious conduct under Federal, State, local, or Tribal law."[161] That is, the bill would just criminalize or further criminalize acts that are already prohibited by law.[162] More recently, Representative Yvette Clarke of New York proposed the "Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019" (the DEEP FAKES Accountability Act of 2019), which would require deepfakers to watermark their videos with

---

158.   TEX. ELEC. CODE ANN. § 255.004 (West 2019).

159.   VA. CODE ANN. § 18.2-386.2(A) (West 2019) VA. CODE ANN. § 18.2-11(a) (West 2019).

160.   CAL. CIV. CODE § 1708.85(b) (West 2020) (providing a private cause of action against persons who create sexually explicit deepfakes); CAL. ELEC. CODE § 20010(a) (West 2020) (prohibiting distribution of deceptive media "with actual malice" within sixty days of an election); K.C. Halm et al., *Two New California Laws Tackle Deepfake Videos in Politics and Porn*, DAVIS WRIGHT TREMAINE LLP (Oct. 14, 2019), https://www.dwt.com/insights/2019/10/california-deepfakes-law [https://perma.cc/CCK6-WSQH]. New York, too, has passed a law providing for a private cause of action against the creators of nonconsensual pornographic images created through what the New York legislature called "digitization," i.e., "deepfakery." N.Y. CIV. RIGHTS LAW § 52-c (McKinney 2021) ("'[D]igitization' means to realistically depict the nude body parts of another human being as the nude body parts of the depicted individual").

161.   Malicious Deep Fake Prohibition Act, S. 3805, 115th Cong. (2018).

162.   *See* Brown, *supra* note 26, at 49.

disclaimers identifying the fakery.[163] The bill would establish criminal penalties, punishable by up to five years in prison, for failure to include disclaimers when there is also intent to cause various harms.[164] Additionally the act would provide for civil penalties of up to $150,000 and would establish a standalone private right of action.[165]

Although these statutes are steps in the right direction, some of them are rather blunt instruments that inadequately differentiate between harmful and non-harmful deepfakes. The Texas statute, for example, provides no exceptions for parodies or other uses that would be protected by the First Amendment.[166] Instead, the statute vaguely requires that the deepfake be created "with the intent to deceive" and "with intent to injure a candidate or influence the result of an election."[167] U.S. Representative Yvette Clarke's proposed DEEP FAKES Accountability Act of 2019 is slightly more nuanced: although its disclaimer requirement could be construed as a form of compelled speech,[168] it provides certain exceptions to the disclosure and watermark requirements to account for parodies and other media where "a reasonable person would not mistake the falsified material activity for actual material activity of the exhibited living person."[169] It does not clarify, however, who bears the burden of establishing that the exception applies, which could lead to either over-disclosure or to stifling parodic free speech by those who do not want to include a disclaimer.[170] More significantly, due to Section 230 of the Communications Decency Act, website owners are likely to remain immunized from secondary liability stemming from the civil causes of action created by these statutes (unless Section 230 is amended), thus hampering their effectiveness.[171]

---

163.   DEEP FAKES Accountability Act, H.R. 3230, 116th Cong. (2019) (as referred to H. Subcomm. Terrorism & Homeland Sec., June 28, 2019).

164.   *Id.*

165.   *Id.*

166.   TEX. ELEC. CODE ANN. § 255.004 (West 2019).

167.   *Id.*

168.   *See, e.g.*, Wooley v. Maynard, 430 U.S. 705 (1977) (finding requirement that New Hampshire license plates bear the state's motto "Live Free or Die" constitutes compelled speech in violation of the First Amendment).

169.   DEEP FAKES Accountability Act, H.R. 3230, 116th Cong. (2019) (as referred to H. Subcomm. Terrorism & Homeland Sec., June 28, 2019).

170.   Hayley Tsukayama et al., *Congress Should Not Rush to Regulate Deepfakes*, ELEC. FRONTIER FOUND. (June 24, 2019), https://www.eff.org/deeplinks/2019/06/congress-should-not-rush-regulate-deepfakes [https://perma.cc/A2D9-G6RS].

171.   *See* 47 U.S.C. § 230.

III. MECHANICS OF A FALSE ASSOCIATION CLAIM

This Part outlines the key elements of a false association claim against a deepfake creator or a website hosting deepfakes: establishing standing, proving the four elements of false association, addressing a First Amendment defense, and establishing secondary liability.

A. STANDING

While there is no requirement that a plaintiff show "use in commerce" of her persona to establish standing under Section 43(a) of the Lanham Act,[172] some courts have required plaintiffs to establish a "commercial interest" in their persona to achieve standing.[173]

In 2014, the Supreme Court held in *Lexmark Int'l, Inc. v. Static Control Components, Inc.* that a plaintiff must establish a "commercial interest in reputation or sales" to come within the "zone of interests" of Section 43(a) to assert a false advertising claim.[174]   Additionally, *Lexmark* required false advertising plaintiffs to show "economic or reputational injury flowing directly from the deception wrought by the defendant's advertising . . . [which] occurs when deception of consumers causes them to withhold trade from the plaintiff."[175] Courts are split on whether *Lexmark*—which concerned a Section 43(a)(1)(B) false advertising claim—also applies to Section 43(a)(1)(A) false association claims: some courts, without explanation, have extended *Lexmark* to false association,[176] while others have limited *Lexmark* to its context—

---

172.   *See, e.g.*, Belmora LLC v. Bayer Consumer Care AG, 819 F.3d 697 (4th Cir. 2016).

173.   MCCARTHY, *supra* note 74, at § 28:17.

174.   Lexmark Int'l, Inc. v. Static Control Components, Inc, 572 U.S. 118, 131–32 (2014).

175.   *Id.* at 133–34.

176.   *See, e.g.*, Lindley v. Puccino's, Inc., No. CV 19-11414, 2019 WL 4673173, at *2 (E.D. La. Sept. 25, 2019) ("Applying those principles [of *Lexmark*] to Lindley's false endorsement claim under § 1125(a), Lindley has demonstrated that she is within the class of plaintiffs authorized to sue under § 1125(a)."); One Source Env't., LLC v. M + W Zander, Inc, No. 2:12-CV-145, 2015 WL 7428572, at *11 (D. Vt. Nov. 20, 2015) (granting summary judgment to defendant on issue of false association because plaintiff failed to show sufficient "injury to a commercial interest in its sales or reputation"); Walkowicz v. American Girl Brands, LLC, No. 20-CV-374-JDP, 2021 WL 510729, at *3 (W.D. Wis. Feb. 11, 2021) (applying *Lexmark*'s commercial-interest requirement to Lanham Act false-endorsement claim). The U.S. District Court for the Northern District of Illinois has inconsistently applied *Lexmark* to false association claims. *Compare* Martin v. Wendy's Int'l, Inc., 183 F. Supp. 3d 925, 932 (N.D. Ill. 2016) (applying *Lexmark* commercial-interest requirement to Lanham Act false-endorsement claim), *and* Yeager v. Innovus Pharm., Inc.,

false advertising.[177] One court, which did not apply *Lexmark* to false association claims, reasoned there is grounding in the opinion of *Lexmark* to limit its standing requirements to false advertising claims.[178] As the U.S. District Court for the District of Maryland noted in *Hershey Co. v. Friends of Steve Hershey*,[179] the Supreme Court in *Lexmark* contrasted false association from false advertising claims, thus appearing to limit its standing requirement to false advertising claims:

> Most of the enumerated purposes [in the Lanham Act, including that of preventing fraud and deception] are relevant to false-association cases; a typical false-advertising case [however] will implicate only the Act's goal of "protect[ing] persons engaged in [commerce within the control of Congress] against unfair competition." Although "unfair competition" was a "plastic" concept at common law, it was understood to be concerned with injuries to business reputation and present and future sales.
>
> We thus hold that to come within the zone of interests in a suit for false advertising under § 1125(a), a plaintiff must allege an injury to a commercial interest in reputation or sales.[180]

No. 18-CV-397, 2019 WL 447743, at *7 (N.D. Ill. Feb. 5, 2019) (same), *with* Ratchford v. AEG Ventures, LLC, No. 17 C 7368, 2019 WL 10248701, at *4 (N.D. Ill. Mar. 11, 2019) (more recently applying *Lexmark* to 1125(a)(1)(B) false advertising claims but not to 1125(a)(1)(A) false association claims). The D.C. Circuit has cited *Lexmark* for the proposition that, to establish the elements of a false association claim (rather than to establish the threshold issue of standing), the plaintiff must prove a commercial interest that could be harmed by infringement, which the U.S. District Court for the District of Columbia interpreted as extending *Lexmark* to 43(a)(1)(A). *See* Abrahams v. Simplify Compliance, LLC, No. CV 19-3009 (RDM), 2021 WL 1197732, at *4 (D.D.C. Mar. 30, 2021) (citing Paleteria La Michoacana, Inc. v. Productos Lacteos Tocumbo S.A. De C.V., 743 F. App'x 457 (D.C. Cir. 2018)).

177.   *See, e.g.*, Avalos v. IAC/Interactivecorp., No. 13-CV-8351(JMF), 2014 WL 5493242, at *4 (S.D.N.Y. Oct. 30, 2014) (applying *Lexmark* to 1125(a)(1)(B) false advertising claims but not to 1125(a)(1)(A) false association claims); Mitchell v. Sanchez, No. 14-0996-CV-ODS, 2015 WL 1393266, at *2 (W.D. Mo. Mar. 25, 2015); Krupa v. Platinum Plus, LLC, No. 8:16-CV-3189-T-33MAP, 2017 WL 1050222, at *5 (M.D. Fla. Mar. 20, 2017); Hershey Co. v. Friends of Steve Hershey, No. WDQ-14-1825, 2015 WL 795841, at *5 (D. Md. Feb. 24, 2015); Gray v. LG&M Holdings LLC, No. CV-18-02543-PHX-SRB, 2020 WL 6200165, at *10 (D. Ariz. Sept. 23, 2020) (applying Lexmark to false advertising claim but not to false association claim); Mitcheson v. El Antro LLC, No. CV-19-01598-PHX-GMS, 2020 WL 7075239, at *15 (D. Ariz. Dec. 3, 2020).

178.   *Hershey Co.*, 2015 WL 795841, at *5.

179.   *Id.*

180.   *Lexmark Int'l, Inc.*, 572 U.S. at 131–32 (citations omitted).

Moreover, imposing heightened standing requirements for false advertising, relative to false association, is consistent with what courts did before *Lexmark*: the Ninth Circuit, for example, historically required false advertising plaintiffs to be direct competitors of defendants but did not impose such a requirement on false association plaintiffs.[181]

Despite the argument *Lexmark* should not extend to false association, it is important to note that even before *Lexmark* was decided in 2014, some courts, including the Ninth Circuit,[182] required plaintiffs to have "at minimum, a present intent to commercialize a mark [i.e., a persona]"[183] and not just a "mere potential of commercial interest"[184] to achieve Section 43(a)(1)(A) standing.

The import of such a commercial interest requirement, whether pre- or post-*Lexmark*, is that it may forbid private persons—individuals who are not public figures or who have insufficient community recognition—from suing under a theory of false association.[185] In *Stayart v. Yahoo! Inc.*, for example, the Seventh Circuit affirmed the denial of standing to a plaintiff who alleged her name had commercial value due to her general involvement in

---

181.   In *Jack Russell Terrier Network of Northern California v. American Kennel Club, Inc.*, now superseded by *Lexmark* with respect to its false advertising holding, the Ninth Circuit explained its different standing requirements for false advertising and false association:

> We have said that different causes of action alleged pursuant to the different subsections of 15 U.S.C. § 1125(a) have different standing requirements. Smith and Waits involved the "false association" prong of § 43 of the Lanham Act, 15 U.S.C. § 1125(a)(1)(A), under which a plaintiff need only allege commercial injury based upon the deceptive use of a trademark or its equivalent to satisfy standing requirements. That the parties be competitors "in the traditional sense" is not required. On the other hand, for standing pursuant to the "false advertising" prong of § 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B), a plaintiff must show: (1) a commercial injury based upon a misrepresentation about a product; and (2) that the injury is "competitive," or harmful to the plaintiff's ability to compete with the defendant.

407 F.3d 1027, 1037 (9th Cir. 2005) (citations omitted).

182.   *Id.*

183.   Condit v. Star Editorial, Inc., 259 F. Supp. 2d 1046, 1052 (E.D. Cal. 2003) (rejecting plaintiff's false endorsement claim, because the plaintiff was a "private figure," and the complaint did not allege "(1) a present intent to use her identity for commercial purposes; (2) any past or existing commercial use of her image and identity, or that it has commercial value; or (3) that she competes commercially in the use of her persona; and (4) has suffered commercial injury to such an interest in her image and identity."). *See also* Dovenmuehle v. Gilldorn Mortg. Midwest Corp., 871 F.2d 697, 700–01 (7th Cir. 1989).

184.   Hutchinson v. Pfeil, 211 F.3d 515, 521 (10th Cir. 2000).

185.   *See Condit*, 259 F. Supp.2d at 1052. The requirement of a commercial interest also precludes a consumer from suing for being misled. *Lexmark Int'l, Inc.*, 572 U.S. at 131–32.

the community, because there was no evidence she was engaged in or anticipated engaging in "the commercial marketing of her identity."[186] Likewise, in *Cohen v. Facebook, Inc.*, a federal district court denied standing, for lack of commercial interest, to non-celebrity Facebook users whose profile photos and names were used by Facebook to promote its "Friend Finder" feature.[187]

Even under the "commercial interest" requirement, however, many individuals targeted by deepfakes have a strong argument for achieving standing under Section 43(a)(1)(A). *Lexmark* is not insurmountable—the Supreme Court clarified in its decision that the plaintiff need not be a competitor of the defendant, and that disparaging remarks can be sufficient to establish proximate causation sufficient for standing.[188] In some cases involving deepfakes, standing will be obvious: professional athletes or celebrities who regularly license their identities to market products can easily establish a commercial interest.[189] Similarly, politicians targeted by deepfakes could argue they have a commercial interest in directing funds to their not-for-profit campaigns, an interest that could be subverted by a confusing

---

186. Stayart v. Yahoo! Inc., 651 F. Supp. 2d 873, 881 (E.D. Wis. 2009), *aff'd*, 623 F.3d 436 (7th Cir. 2010) (denying standing to plaintiff whose false endorsement suit alleged that Yahoo! users would believe she was associated with or endorsed unsavory results stemming from a Yahoo! search of her name, "Bev Stayart."). *See also* Nieman v. Versuslaw, Inc., No. 12-3104, 2012 WL 3201931, at *5 (C.D. Ill. Aug. 3, 2012), *aff'd*, 512 F. App'x 635 (7th Cir. 2013) (denying standing to plaintiff, a private person and insurance claims adjuster, who similarly based his theory of false endorsement on search results for his name on legal search websites like Versuslaw and Lexis/Nexis).

187. Cohen v. Facebook, Inc., 798 F. Supp. 2d 1090, 1097–98 (N.D. Cal. 2011). Notably, in both *Stayart* and *Cohen*, the plaintiffs were unlikely to establish a likelihood of confusion, even if they did show a "commercial interest" in their identities. In *Stayart*, the court actually found there was no likelihood of confusion: "Even if Stayart is engaged in commercial activity with respect to her identity, a commonsense reading of the complaint demonstrates that there could be no likelihood of confusion." *Stayart*, 651 F. Supp. 2d at 883. In *Cohen*, the court made no such finding, but the facts were similarly disfavorable for a likelihood of confusion: Facebook's promotion of its Friend Finder service merely indicated certain Facebook members had used the service; the promotion did not indicate the users endorsed or affirmatively chose to associate with Facebook's messaging about the Friend Finder service. *See generally Cohen*, 798 F. Supp. 2d, at 1095–98.

188. Lexmark Int'l, Inc. v. Static Control Components, Inc, 572 U.S. 118, 138 (2014) ("When a defendant harms a plaintiff's reputation by casting aspersions on its business, the plaintiff's injury flows directly from the audience's belief in the disparaging statements.").

189. *See, e.g.*, Kournikova v. Gen. Media Commc'ns Inc., 278 F. Supp. 2d 1111, 1120 (C.D. Cal. 2003) (granting Section 43(a) standing to celebrity tennis player). Although it will be easier for celebrities to show a commercial interest in their identities, even courts requiring a commercial interest have held Section 43(a) "does not have a requirement that a plaintiff is a celebrity." Arnold v. Treadwell, 642 F. Supp. 2d 723, 735 (E.D. Mich. 2009) (plaintiff had commercial interest where she "introduced evidence showing a present intent to commercialize her identity" and "offered evidence that she has sought modeling jobs.").

deepfake. Indeed, courts have held that the use of a persona for charitable endeavors constitutes a commercial interest.[190] Further, even courts purporting to impose a commercial interest requirement have sometimes allowed non-celebrities to proceed with their claims.[191] Hence, a commercial interest requirement, though an obstacle, need not impede false association suits by deepfake victims, celebrity or not.

B. ASSERTING A PRIMA FACIE CLAIM OF FALSE ASSOCIATION

To prevail on a false association claim, a plaintiff must establish that the defendant, (i) in commerce, (ii) in connection with goods or services, (iii) made a false or misleading representation of fact (iv) that is likely to cause consumer confusion as to the origin, sponsorship, or approval of goods or services.[192] Of these four elements of infringement, the second—use in connection with goods or services—is likely to be the most difficult to establish in the context of deepfakes.

---

190.   Cairns v. Franklin Mint Co., 24 F. Supp. 2d 1013, 1033 (C.D. Cal. 1998) (For the purposes of establishing "commercial interest" for Section 43(a) standing, it was "immaterial" that the plaintiff used profits for charitable purposes; the plaintiff—a deceased celebrity's estate and charitable fund—had a "commercial interest" for the purposes of Section 43(a), because defendant's use of the celebrity's persona would confuse consumers as to whether the plaintiff endorsed the defendant's products.).

191.   *See* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 306 n.20 (D.N.H. 2008) (denying defendant's motion to dismiss false association claim, where the plaintiff was a non-celebrity who did not allege she commercialized or intended to commercialize her persona, reasoning that damage to commercial value can be presumed when the defendant uses the plaintiff's persona in an advertisement without permission). *But see* Stayart v. Yahoo! Inc., 651 F. Supp. 2d 873, 881 (E.D. Wis. 2009), *aff'd*, 623 F.3d 436 (7th Cir. 2010) (distinguishing *Friendfinder Network* on the grounds that it did not explicitly discuss the issue of prudential standing, reasoning that a court is not obliged to raise questions of prudential standing).

192.   Burck v. Mars, Inc., 571 F. Supp. 2d 446, 455 (S.D.N.Y. 2008), cited by, e.g., Toth v. 59 Murray Enterprises, Inc., No. 15 CIV. 8028 (NRB), 2019 WL 95564, at *5 (S.D.N.Y. Jan. 3, 2019), *aff'd in part sub nom.* Electra v. 59 Murray Enterprises, Inc., 987 F.3d 233 (2d Cir. 2021)). *See also* 15 U.S.C. § 1125(a)(1)(A).

1. *Use in Commerce*

As a threshold matter, it is crucial to note the "use in commerce" and "in connection with any goods or services" elements are distinct,[193] although courts have at times conflated the two.[194] "Use in commerce" is a jurisdictional term referring broadly to Congress' intent to legislate using its Commerce Power, while "in connection with any goods or services" limits the types of uses that can constitute actionable infringement.[195]

Courts have interpreted the "use in commerce" requirement of Section 43(a) "to refer to a use that falls within Congress's commerce power."[196] Although the Lanham Act itself defines "use in commerce," courts have generally not applied this definition in the context of infringement. As McCarthy explains:

> Under any of the three bases for recovery (registered or unregistered infringement and dilution), the Lanham Act requires that the plaintiff prove that the accused party has made a "use in commerce" of the accused mark. It has been argued that the Lanham Act § 45 definition of "use in commerce" is in effect a statutory requirement that the accused use be a "trademark" use. Lanham Act § 45 defines

---

193. *See, e.g.*, United We Stand Am., Inc. v. United We Stand, Am. N.Y., Inc., 128 F.3d 86, 89 (2d Cir. 1997) (analyzing "use in commerce" and "in connection with any goods or services" separately); Radiance Found., Inc. v. NAACP, 786 F.3d 316, 322 (4th Cir. 2015) ("An actionable trademark claim does not simply require that the alleged infringer used in commerce the mark that the trademark holder possesses. It also requires that the infringer's use be 'in connection with' goods or services in a manner that is 'likely to cause confusion'. . . ."); Utah Lighthouse Ministry v. Found. for Apologetic Info. & Rsch., 527 F.3d 1045, 1054 (10th Cir. 2008) ("It is important to distinguish between the merely jurisdictional 'in commerce' requirement, *see* 15 U.S.C. § 1127, and the 'in connection with any goods and services' requirement that establishes a violation of section 43 of the Lanham Act.").

194. Bosley Med. Inst., Inc. v. Kremer, 403 F.3d 672, 677 (9th Cir. 2005), *aff'd in part, rev'd in part*, 403 F.3d 672 (9th Cir. 2005). In that case, the court stated:

> The district court ruled that Kremer's use of Bosley's mark was noncommercial. To reach that conclusion, the court focused on the "use in commerce" language rather than the "use in connection with the sale of goods" clause. This approach is erroneous. "Use in commerce" is simply a jurisdictional predicate to any law passed by Congress under the Commerce Clause. . . . Therefore, the district court should have determined instead whether Kremer's use was "in connection with a sale of goods or services" rather than a "use in commerce."

Id.

195. *See Burck*, 571 F. Supp. at 454; 15 U.S.C. § 1125(a)(1)(A).

196. Rescuecom Corp. v. Google Inc., 562 F.3d 123, 138 (2d Cir. 2009). *See also* Lens.com, Inc. v. 1-800 Contacts, Inc., 686 F.3d 1376, 1380 (Fed. Cir. 2012) (interpreting "use in commerce" as a jurisdictional predicate indicating Congress's intent to legislate to the limits of its Commerce Clause authority).

a "use in commerce" as being limited either to certain kinds of use on goods or use in the sale or advertising of services. In my view this is not a reasonable reading of the statute. The Lanham Act § 45 definition of "use in commerce" is limited to certain defined kinds of use such as on "displays associated" with the goods or on "tags or labels." It was clearly drafted to define the types of "use" that are needed to qualify a mark for federal registration—not as a candidate for infringement. It defines the kinds of "use" needed to acquire registerable trademark rights—not to infringe them. . . .

[T]he Second, Ninth and Federal Circuits agree with the author's position as described above: the Lanham Act § 45 definition of "use in commerce" defines the kind of use needed to register a mark, not to infringe it.[197]

Hence, most courts have held plaintiffs are "not required to demonstrate that a defendant made use of the mark in any particular way to satisfy the 'use in commerce' requirement."[198]

In *Rescuecom Corp. v. Google Inc.*, the Second Circuit prominently employed this broad construction of "use in commerce."[199] At issue in *Rescuecom* was Google's AdWords program, which lets advertisers pay for their websites to appear as search results in response to searches for specific keywords.[200] In the case of *Rescuecom*, Google's Keyword Suggestion Tool had recommended the keyword (and plaintiff's trademark), RESCUECOM, to Rescuecom's competitors, who purchased the keyword so their advertisements would appear when users

---

197. MCCARTHY, *supra* note 74, at § 23:11.50 (5th ed. 2021) (citing *Rescuecom Corp.*, 562 F.3d at 139; *Bosley Med. Inst., Inc.*, 403 F.3d at 677; VersaTop Support Systems, LLC v. Georgia Expo, Inc., 921 F.3d 1364, 1370 (Fed. Cir. 2019)). The Sixth Circuit has more narrowly interpreted the "use in commerce" provision to require "trademark use." *Id.* (citing, e.g., Interactive Products Corp. v. a2z Mobile Office Solutions, Inc., 326 F.3d 687, 695 (6th Cir. 2003) ("If defendants are only using [plaintiff's] trademark in a 'non-trademark' way—that is, in a way that does not identify the source of a product—then trademark infringement and false designation of origin laws do not apply."). One rationale for the Sixth Circuit's interpretation, noted by McCarthy, is that non-trademark use of a mark is less likely to trigger a likelihood of confusion. *Id.*

198. Kelly-Brown v. Winfrey, 717 F.3d 295, 305 (2d Cir. 2013).

199. *Rescuecom Corp.*, 562 F.3d at 124.

200. *Id.* at 125–27. Google's AdWords program is now called "Google Ads." *Google AdWords is now Google Ads*, GOOGLE ADS HELP (2021), https://support.google.com/google-ads/answer/9028765 [https://perma.cc/XD2B-PM8F].

searched for "Rescuecom."[201] The plaintiff, Rescuecom, based its infringement claim on its allegation that Google users would be misled to believe that the advertisements appearing in response to searches for "Rescuecom" were affiliated with or endorsed by the plaintiff.[202] The court held defendant Google's sale of keywords to advertisers through its AdWords program constituted a "use in commerce," even though the keyword (plaintiff's mark, RESCUECOM) in dispute was not actually displayed to users of Google in connection with the competitors' links.[203] This contrasts with the case of deepfakes, where the plaintiffs' marks, their personas, are displayed prominently in the infringing media—the deepfake videos themselves.

Generally, plaintiffs in deepfake suits will have a strong argument that deepfakes fall under Congress' Commerce Clause authority: deepfakes are shared nationally on websites like YouTube and Facebook, and widely disseminated videos of public figures or political leaders are likely to incite responses unconstrained by state lines.[204] Even if a deepfake is not widely distributed across state lines, deepfakes targeting political figures, for example, may affect their target's ability to raise campaign funds or to market their identities for other purposes.[205] In *Planned Parenthood Federation of America, Inc. v. Bucci*, for example, the Second Circuit held that defendant Bucci's use of the "plannedparenthood.com" domain name met the "use in commerce" requirement even if defendant's activities alone did not

---

201. *Id.* Although the court held the use in commerce element was established, it was unlikely the plaintiff could establish a likelihood of confusion. *See, e.g.*, Network Automation, Inc. v. Advanced Sys. Concepts, Inc., 638 F.3d 1154 (9th Cir. 2011) (on similar facts to *Rescuecom*, reversing district court's preliminary injunction against Network Automation, reasoning that Advanced System's "showing of a likelihood of confusion was insufficient). Indeed, the Ninth Circuit expressed no opinion on the likelihood of confusion in *Rescuecom*. 562 F.3d at 130 ("We have no idea whether Rescuecom can prove that Google's use of Rescuecom's trademark in its AdWords program causes likelihood of confusion or mistake.").

202. *Rescuecom Corp.*, 562 F.3d at 125–27.

203. *Id.* at 127.

204. *See* Planned Parenthood Fed'n of Am., Inc. v. Bucci, No. 97 Civ 0629 (KMW), 1997 WL 133313, at *3 (S.D.N.Y. Mar. 24, 1997) ("Internet users constitute a national, even international, audience, who must use interstate telephone lines to access defendant's web site on the internet. The nature of the internet indicates that establishing a typical home page on the internet, for access to all users, would satisfy the Lanham Act's 'in commerce' requirement."), *aff'd*, 152 F.3d 920 (2d Cir. 1998); MCCARTHY, *supra* note 74, at § 25:54.50 ("When an alleged infringing mark is used on the internet, the use is clearly a 'use in commerce' that can be regulated by the Lanham Act under the Constitution.").

205. *See Planned Parenthood Fed'n of Am., Inc.*, 1997 WL 133313, at *3.

directly constitute interstate commerce: "even assuming, arguendo, that defendant's activities are not in interstate commerce for Lanham Act purposes, the effect of those activities on plaintiff's interstate commerce activities would place defendant within the reach of the Lanham Act." Deepfakes employing the personas of others, then, can fall within Section 43's "use in commerce" requirement, either by way of their mass viewership on the internet or their effects on the plaintiff.

2. *In Connection with Any Goods or Services*

Courts have generally read the "in connection with any goods or services" requirement broadly, applying Section 43(a) to "defendants furnishing a wide variety of non-commercial public and civic benefits."[206] However, courts sometimes apply a narrower version of it, referring to the "in connection with" requirement as a "commercial use" requirement,[207] which might be challenging for a plaintiff to meet in the context of deepfakes. This narrower interpretation is contradicted by the text of the Lanham Act, as Section 43(a)(1)(A) (false association)[208] does not limit itself to infringing uses that are commercial, in contrast to Section 43(a)(1)(B) (false advertising)[209] and Section 43(c) (dilution).[210]

Nonetheless, despite Section 43(a)(1)(A)'s silence on the commerciality of the defendant's activities, some courts have imposed this narrower "commercial use" requirement on false association claims.[211] The Fourth Circuit, for example, has applied a non-exclusive three factor "commercial speech" test for deciding whether a defendant's use of a mark is commercial, which considers: "whether the speech is an advertisement; whether the

206.   United We Stand Am., Inc. v. United We Stand, Am. N.Y., Inc., 128 F.3d 86, 90 (2d Cir. 1997) (collecting cases); SMJ Grp., Inc. v. 417 Lafayette Rest. LLC, 439 F. Supp. 2d 281, 287 (S.D.N.Y. 2006).

207.   *See* MCCARTHY, *supra* note 74, at § 23:11.50 (citing, e.g., Keel v. Axelrod, 148 F. Supp. 3d 411, 419 (E.D. Pa. 2015)).

208.   *See* 15 U.S.C § 1125(a)(1)(A).

209.   *See* 15 U.S.C § 1125(a)(1)(B) (restricting itself to "commercial advertising or promotion"). *See also* McCarthy, MCCARTHY, *supra* note 74, at § 27:71 (similarly noting there is no requirement of commerciality in Section 43(a)(1)(A)).

210.   *See* 15 U.S.C § 1125(c)(3)(C) ("any noncommercial use of a mark" is "not actionable as dilution").

211.   *See, e.g.*, Radiance Found., Inc. v. NAACP, 786 F.3d 316, 323 (4th Cir. 2015) ("Although this case does not require us to hold that the commercial speech doctrine is in all respects synonymous with the "in connection with" element, we think that doctrine provides much the best guidance in applying the Act.").

speech references a particular good or service; and whether the speaker (the alleged infringer) has a demonstrated economic motivation for his speech."[212] Although non-profit uses of a mark can still be found actionable,[213] the commercial use requirement tends to generally limit the applicability of Section 43(a).[214] Courts applying a narrower commerciality requirement have rationalized it as an added protection against intrusion upon First Amendment values.[215] However, in addition to the fact that a "commercial use" requirement does not have a basis in the text of Section 43(a) and many courts do not apply it,[216] it is arguably unnecessary to impose a "commercial use" requirement for First Amendment purposes, since courts already apply the very robust *Rogers* test (as a defense to infringement) to protect against intrusion on the First Amendment.[217]

Despite the questionable merits of a robust interpretation of the "in connection with any goods or services" requirement, the fact that some courts apply it presents a hurdle to Section 43(a) claims

---

212. *Id.* (stating "[t]hese are not exclusive factors, and the presence or absence of any of them does not necessitate a particular result.") (citing Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 66–67 (1983)).

213. *See* Valley Forge Military Acad. Found. v. Valley Forge Old Guard, Inc., 24 F. Supp. 3d 451, 455 (E.D. Pa. 2014) (applying the same three-factor commercial speech test and granting standing to sue for infringement against a non-profit provider of alumni services).

214. *Compare* People for Ethical Treatment of Animals v. Doughney, 263 F.3d 359, 365 (4th Cir. 2001) (not applying a commercial use test and allowing infringement action to proceed against defendant using plaintiff's mark in its peta.org domain name), *with* Bosley Med. Inst., Inc. v. Kremer, 403 F.3d 672, 679 (9th Cir. 2005) (on very similar facts to *Doughney*, applying a commercial use test and disallowing an infringement claim based on defendant's use of plaintiff's BOSLEY MEDICAL mark in its BosleyMedical.com domain name). Of note, the Fourth Circuit, since *Doughney*, has applied the commercial use test. *See Radiance Found.*, 786 F.3d at 323. This footnote compares *Doughney* with *Bosley* not to highlight a circuit split, but to show how two very similar cases were decided differently when the courts applied differing "in connection with" doctrines.

215. *See Radiance Found.*, 786 F.3d at 322 ("At the very least, reading the 'in connection with' element to take in broad swaths of noncommercial speech would be an 'overextension' of the Lanham Act's reach that would 'intrude on First Amendment values.'").

216. *See, e.g.*, United We Stand Am., Inc. v. United We Stand, Am. N.Y., Inc., 128 F.3d 86, 90 (2d Cir. 1997); SMJ Grp., Inc. v. 417 Lafayette Rest. LLC, 439 F. Supp. 2d 281, 287 (S.D.N.Y. 2006) (Where the alleged infringing use was in leaflets raising awareness of restaurant employees' work conditions, the court held the defendant's use was in connection with a public "service," stating that "defendants' lack of profit motivation does not place their activities beyond the scope of the Lanham Act's definition of 'services.'"); Brach Van Houten Holding, Inc. v. Save Brach's Coal. for Chicago, 856 F. Supp. 472, 475–76 (N.D. Ill. 1994) (collecting cases, and holding that defendant's "soliciting donations, preparing press releases, . . . [and engaging in other] work on behalf of its members' interests constitutes a 'service' within the meaning of the Lanham Act.").

217. *See* Rogers v. Grimaldi, 875 F.2d 994, 999 (2d Cir. 1989). *See also* Lemley, *supra* note 96, at 1173 (discussing how *Rogers* limits Lanham Act claims and collecting cases).

involving deepfakes. In *Radiance Foundation, Inc. v. N.A.A.C.P.*, for example, at issue was whether Radiance Foundation's article, entitled, "NAACP: National Association for the Abortion of Colored People," infringed the NAACP mark.[218] The article criticized the NAACP for sponsoring an event Radiance alleged "defied Christian values."[219] On the side of the webpage featuring the article was a "Donate" button allowing viewers to contribute to the Radiance Foundation, a Christian organization.[220] Despite the "Donate" button, the Fourth Circuit, applied a narrower, commercial use-focused version of the "in connection with" requirement,[221] and held Radiance Foundation's use of the NAACP's marks could not support Lanham Act liability, because the use was "noncommercial."[222] The court reasoned that the use of the NAACP mark "was too attenuated from the donation solicitation" and did not seem to "denote the recipient of the donation."[223]

Somewhat similarly, in *Bosley Med. Inst., Inc. v. Kremer*, the Ninth Circuit held that "noncommercial use of a trademark as the domain name of a website" was not actionable under the Lanham Act.[224] At issue in *Bosley* was the defendant Kremer's use of the plaintiff's mark in his website's domain name, www.BosleyMedical.com, which heavily criticized the plaintiff's business.[225] The court characterized defendant's use of the mark as noncommercial—"merely . . . to identify the object of consumer criticism"—and held it was nonactionable.[226] In the vein of cases like *Radiance Foundation* and *Bosley*, a deepfake creator can argue their use of a plaintiff's likeness is too removed from any commercial hook such as advertisements featured on the webpage or links to other sites offering goods or services.

One common thread of *Radiance Foundation* and *Bosley*, however, that distinguishes them from deepfakes is that confusion

---

218. *Radiance Found., Inc.*, 786 F.3d at 319.
219. *Id.* at 320.
220. *Id.* at 326.
221. *Id.* at 323 (applying a three-part commercial speech test from *Bolger*) (citing Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 66–67 (1983)).
222. *Id.* at 326.
223. *Id.* at 327. The court reasoned that "[s]uch a nexus [between the use of the mark and the good/service] may be present, for example, where the protected mark seems to denote the recipient of the donation," which was not true in the case at hand. *Id.*
224. Bosley Med. Inst., Inc. v. Kremer, 403 F.3d 672, 674 (9th Cir. 2005).
225. *Id.*
226. *Id.* at 679.

was very unlikely. In *Radiance Foundation*, the court actually found there was no likelihood of confusion: "The critical message conveyed by the satirical mark itself and in the commentary that follows ensures that no confusion about the source of the commentary will last, if in fact it is generated at all."[227] Similarly, in *Bosley*, the district court held there was no likelihood of confusion where the defendant's webpage, which blatantly criticized plaintiff *Bosley*, was unlikely to mislead consumers.[228]

Even if a court were to apply the commercial use-focused interpretation of the "in connection with any goods or services" requirement discussed above, plaintiffs in deepfake suits have arguments for bringing deepfakes within the Lanham Act's province.

As a threshold matter, deepfakes themselves may constitute "goods or services" since they are videos from which their creators can derive profits.[229] Indeed, courts have held that Section 43(a) "does not require that the mark be used in connection with separate goods to promote the purchase of those separate goods— but may be used directly on the defendant's goods."[230]

In *Fifty-Six Hope Road Music, Ltd. v. A.V.E.L.A., Inc.*, for example, the Ninth Circuit upheld a jury verdict of false association, where the defendant used Bob Marley's image directly on its merchandise without authorization.[231] In the case of deepfakes, YouTube, Facebook, and other sites to which deepfakes may be posted allow video-posters to monetize their content by

---

227.   *Radiance Found., Inc.*, 786 F.3d at 328.

228.   Bosley Med. Inst., Inc. v. Kremer, No. Civ.01-1752WQHJMA, 2004 WL 964163, at *8 (S.D. Cal. Apr. 30, 2004), *aff'd in part, rev'd in part and remanded*, 403 F.3d 672 (9th Cir. 2005). On appeal, the Ninth Circuit did not reach the issue of likelihood of confusion (or initial interest confusion, for which there was a good argument), because it found the defendant's use was non-infringing as a threshold matter because it was noncommercial. *Bosley Med. Inst., Inc.*, 430 F.3d at 680 n.3.

229.   *See, e.g.*, Naked Cowboy v. CBS, 844 F. Supp. 2d 510, 513 (S.D.N.Y. 2012) (allowing false endorsement claim to proceed against CBS, where subject of dispute was a YouTube video) (quoting Fifty-Six Hope Road Music, Ltd. v. A.V.E.L.A., Inc., 778 F.3d 1059, 1072 (9th Cir. 2015), *cert. denied*, 577 U.S. 957 (2015)).

230.   MCCARTHY, *supra* note 74, at § 28:15 ("False endorsement cases under Lanham Act § 43(a) are not limited to a use of the plaintiff's identity in advertising to sell goods or services, but also includes unpermitted use of plaintiff's identity on a product itself, as with a name or image on a t-shirt or poster.").

231.   Fifty-Six Hope Road Music, Ltd. v. A.V.E.L.A., Inc., 778 F.3d 1059, 1072 (9th Cir. 2015), *cert. denied*, 577 U.S. 957 (2015). *See also, e.g.*, Bruce Lee Enterprises, LLC v. A.V.E.L.A., Inc., No. 10 CV 2333 KMW, 2013 WL 822173 (S.D.N.Y. Mar. 6, 2013) (denying defendant's motion for summary judgment on false endorsement based on defendant's unauthorized licensing of martial artist Bruce "Lee's image for use on a variety of products, including t-shirts, posters, and bobblehead dolls.").

sharing in the revenue generated from advertisements displayed in conjunction with their videos.[232] Facebook also allows the owners of Facebook pages to charge for online events and to generate subscription revenue by providing exclusive content.[233] Unlike in *Radiance*, the owner of a social media page featuring deepfakes may, as a direct result of the confusion caused by the videos, profit via advertising revenue from viewership. Deepfakes displayed in conjunction with profit-making channels like ad revenue-sharing are more likely to trigger Section 43(a)'s "in connection with any goods or services" requirement even under a narrower formulation of it, because they are economically motivated.[234] Moreover, some courts have held "[e]ven 'extremely minimal' commercial activity, such as providing a link to a third-party website that sells goods, can trigger liability."[235] Thus, the presentation of deepfakes in conjunction with links to commercial sites may be sufficient to meet the narrow, commercial use-focused interpretation of the "in connection with any goods or services" requirement.

In other contexts, it may be more difficult to establish the "in connection with any goods or services" element, since deepfakes can be uploaded by anonymous trolls unassociated with a revenue-generating social media account or with a website containing commercial links. However, even deepfakes without a

---

232. *YouTube Partner Earnings Overview*, YOUTUBE HELP, https://support.google.com/youtube/answer/72902?hl=en#zippy=%2Chow-do-i-get-paid [https://perma.cc/AN3K-MBAP]; *How Can I Make Money on Facebook?*, FACEBOOK BLUEPRINT, https://www.facebook.com/business/learn/lessons/how-make-money-facebook [https://perma.cc/P7A4-354H] [hereinafter FACEBOOK].

233. FACEBOOK, *supra* note 232.

234. *Radiance Found.*, 786 F.3d at 323 (considering "economic motivation" as one factor weighing in favor of a finding of "commercial speech" for the purposes of the "in connection with" goods or services requirement).

235. XPO CNW, Inc. v. R+L Carriers, Inc., No. 16-10391, 2016 WL 4801283, at *3 (E.D. Mich. Sept. 14, 2016) (quoting Taubman Co. v. Webfeats, 319 F.3d 770, 775 (6th Cir. 2003)); Int'l Bhd. of Teamsters Loc. 651 v. Philbeck, 423 F. Supp. 3d 364, 373–74 (E.D. Ky. 2019) (denying motion to dismiss where the defendant used the plaintiff's marks on a Facebook page in conjunction with links to third-party sites selling goods and services, stating "Philbeck's provision of links for discounts to Union members serves to meet the extremely minimal bar for commercial activity."); People for Ethical Treatment of Animals v. Doughney, 263 F.3d 359, 366 (4th Cir. 2001) (finding it favorable to the plaintiff, for the purposes of establishing the "in connection with" element, that the defendant's site provided links "to more than 30 commercial operations offering goods and services," even though these links did not direct the viewer to webpages operated by the defendant). *See also* Bell v. Worthington City Sch. Dist., No. 2:18-CV-961, 2020 WL 2905803, at *17 (S.D. Ohio June 2, 2020) ("including advertising links on an otherwise non-commercial website falls within the Lanham Act.").

"commercial" hook as obvious as YouTube advertisement revenue may still be actionable under other theories of the "in connection with" provision. Some courts, for example, have allowed infringement claims to proceed based on an argument that the defendant's use of a mark diverted consumers from the plaintiffs' goods or services. In *People for Ethical Treatment of Animals v. Doughney*, at issue was defendant Doughney's use of the peta.org domain name for a website he titled, "People Eating Tasting Animals," which was a "resource for those who enjoy eating meat, wearing fur and leather, [and] hunting."[236] The Fourth Circuit held:

> To use PETA's Mark "in connection with" goods or services, Doughney need not have actually sold or advertised goods or services on the www.peta.org website. Rather, Doughney need only have prevented users from obtaining or using PETA's goods or services, or need only have connected the website to other's goods or services.[237]

Similarly, deepfakes targeting celebrities may divert consumers from the celebrities' profit-making social media profiles or other activities by damaging their reputations, and deepfakes targeting political figures may divert funds from their campaigns as a result of presenting them in a false or misleading manner.

Although a theory of harm based on distortion of the political process does not fit neatly within the mold of a typical Lanham Act

---

236. *Doughney*, 263 F.3d at 363.
237. *Id.* at 365.; *contra* Bosley Med. Inst., Inc. v. Kremer, 403 F.3d 672, 679 (9th Cir. 2005). In *Bosley*, the court stated:

> To the extent that the PETA court held that the Lanham Act's commercial use requirement is satisfied because the defendant's use of the plaintiff's mark as the domain name may deter customers from reaching the plaintiff's site itself, we respectfully disagree with that rationale. . . . We hold today that the noncommercial use of a trademark as the domain name of a website—the subject of which is consumer commentary about the products and services represented by the mark—does not constitute infringement under the Lanham Act.

Id. The Fourth Circuit later distinguished *Doughney* by stating it "applies specifically where the infringer has used the trademark holder's mark in a domain name." *Radiance Found., Inc.*, 786 F.3d at 326. However, in *Radiance Foundation*, as discussed previously, the court found no likelihood of confusion, so its finding of non-commerciality was not necessary for its holding. *See id.* at 328. Moreover, the Fourth Circuit's limiting of *Doughney* to domain names would not prevent a later extension of *Doughney* to the context of deepfakes.

claim,[238] courts have at times articulated a broad interpretation of the "in connection with" requirement for the purposes of protecting the public from confusion during the political process. At issue in *United We Stand America, Inc. v. United We Stand, America New York, Inc.* was a service mark, "United We Stand America," which Ross Perot first used in his 1992 presidential campaign, but which defendant Alex Rodriguez subsequently used in his own political activities.[239] The Second Circuit held that the defendant's political activities constituted "services" for the purposes of the Lanham Act, reasoning:

> Any group trading in political ideas would be free to distribute publicity statements, endorsements, and position papers in the name of the "Republican Party," the "Democratic Party," or any other. The resulting confusion would be catastrophic; voters would have no way of understanding the significance of an endorsement or position taken by parties of recognized major names. The suggestion that the performance of such functions is not within the scope of "services in commerce" seem to us to be not only wrong but extraordinarily impractical for the functioning of our political system.[240]

Even though a deepfake's appropriation of a mark may not directly benefit the creator of the deepfake, it can lead to similar confusion among consumers and voters, and, as discussed above, may divert funding from the target's political campaign. Moreover, since there is no requirement in Section 43(a)(1)(A) that the defendant actually profited for the purposes of establishing infringement, a claim based on the theory of diversion is not foreclosed by the statute.[241]

 In sum, although the "in connection with any goods or services" requirement of Section 43(a)(1)(A) is perhaps the greatest hurdle to a claim against the creators of deepfakes, there are ways to link

---

238.   MCCARTHY, *supra* note 74, at § 5:4 (discussing the protection of consumers and businesses but not of the political process as the intent of the Lanham Act).

239.   *See* United We Stand Am., Inc. v. United We Stand, Am. N.Y., Inc., 128 F.3d 86, 88 (2d Cir. 1997).

240.   *Id.* at 90.

241.   *See* 15 U.S.C. § 1125. A plaintiff failing to show defendant's profits would instead be required to establish her damages resulting from the infringement. *See* 15 U.S.C. § 1117(a).

deepfakes to goods and services by establishing the defendant's economic motivation or by demonstrating how the deepfake diverted consumers from the plaintiff's goods or services.

3. *False or Misleading Representation of Fact*

The remaining two elements—that of a false or misleading representation of fact and that of a likelihood of causing consumer confusion as to the origin, sponsorship, or approval of goods or services—are easier for deepfakes to meet than the "in connection with any goods or services" element.

The "misleading representation" element, in particular, is easy to meet in the context of deepfakes, with courts often glossing over it.[242] In *White v. Samsung Elecs. Am., Inc.*, for example, Vanna White, hostess of "Wheel of Fortune" sued Samsung under Section 43(a)(1)(A) for using a "Vanna White robot" in its advertisements without obtaining her consent.[243] Even though the allegedly infringing content was a robot depiction of White, and therefore arguably less of a misrepresentation than if it were a photo (or deepfake) of White, the Ninth Circuit did not discuss the issue of misrepresentation and instead focused on the likelihood of confusion element.[244] In the case of a deepfake, it would be easy to establish the "misleading representation" element, because deepfakes are misleading by their very nature. Context or disclaimers may signal to the viewer the misleading representation in order to mitigate the likelihood of confusion, but this is addressed by the likelihood of confusion element rather than the misleading representation element.[245]

---

242. *See, e.g.*, Bruce Lee Enterprises, LLC v. A.V.E.L.A., Inc., No. 10 CV 2333 KMW, 2013 WL 822173, at *3, *19 (S.D.N.Y. Mar. 6, 2013) (denying defendant's motion for summary judgment on false endorsement, and glossing over the "false or misleading representation" element, where defendant engaged in unauthorized licensing of martial artist Bruce "Lee's image for use on a variety of products, including t-shirts, posters, and bobblehead dolls.").

243. White v. Samsung Elecs. Am., Inc., 971 F.2d 1395, 1396 (9th Cir. 1992) ("The ad depicted a robot, dressed in a wig, gown, and jewelry which Deutsch consciously selected to resemble White's hair and dress. The robot was posed next to a game board which is instantly recognizable as the Wheel of Fortune game show set, in a stance for which White is famous."). *See also* Wendt v. Host Int'l, Inc., 125 F.3d 806 (9th Cir. 1997) (reversing summary judgment against plaintiff actors on false endorsement where defendant sold robots based on actors' likenesses).

244. *See id.* at 1399.

245. MᴄCᴀʀᴛʜʏ, *supra* note 74, at § 19:72.

4. *Likelihood of Confusion*

False association's likelihood of confusion element originates from the portion of Section 43(a) prohibiting false or misleading representations "likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person."[246] As discussed infra in Part II.A, confusion is the "keystone" and "heart" of a claim under the Lanham Act.[247]

Courts generally apply multi-factor tests, which differ slightly based on the circuit, to find a likelihood of confusion.[248] In *Downing v. Abercrombie & Fitch*, the Ninth Circuit crafted a test specific to false association claims, which considers the following eight factors:

1) The level of recognition that the plaintiff has among the segment of the society for whom the defendant's product is intended;
2) The relatedness of the fame or success of the plaintiff to the defendant's product;
3) The similarity of the likeness used by the defendant to the actual plaintiff;
4) Evidence of actual confusion;
5) Marketing channels used;
6) Likely degree of purchaser care;
7) Defendant's intent on selecting the plaintiff; and
8) Likelihood of expansion of the product lines.[249]

---

246.   15 U.S.C. § 1125(a).

247.   MCCARTHY, *supra* note 74, at § 23:1; Allen v. Nat'l Video, Inc., 610 F. Supp. 612, 627 (S.D.N.Y. 1985) (quoting Standard & Poor's Corp. v. Commodity Exch., Inc., 683 F.2d 704, 708 (2d Cir. 1982)).

248.   *See, e.g.*, Polaroid Corp. v. Polarad Elecs. Corp., 287 F.2d 492, 128 (2d Cir. 1961) (providing the basis for the Second Circuit *Polaroid* likelihood of confusion factors). *See also* MCCARTHY, *supra* note 74, at § 23:19 (discussing the different factors courts use to find a likelihood of confusion).

249.   Downing v. Abercrombie & Fitch, 265 F.3d 994, 1007–08 (9th Cir. 2001) (citing AMF Inc. v. Sleekcraft Boats, 599 F.2d 341, 348–49 (9th Cir. 1979) (retooling the Sleekcraft factors, which the Ninth Circuit traditionally applies to find a likelihood of confusion, for the context of a false endorsement claim). Modified versions of the *Downing* test have also been adopted by other circuits. *See* Facenda v. N.F.L. Films, Inc., 542 F.3d 1007, 1020 (3d Cir. 2008); MCCARTHY, *supra* note 74, at § 28:15.

These factors are highly case-specific and are neither of equal importance nor applicable to every case.[250] So, this Part will focus on those factors most likely to raise difficulties when applied to deepfakes. The first factor, "level of recognition," in particular, has the potential to limit false association claims to those by public figures,[251] but courts have not strictly required "celebrity" status to bring false association actions: "there is a level of consumer recognition short of celebrity—as the term is usually understood—capable of causing consumer confusion."[252] Despite this, private citizens generally unknown to the public may have trouble establishing infringement claims for at least two reasons: viewers are less likely to be deceived into watching a deepfaked video featuring unknown individuals, and viewers are unlikely to be confused by a persona that is unrecognizable and therefore not meaningful to them.[253]

Additionally, the second factor, "relatedness of the fame or success of the plaintiff to the defendant's product," is not obviously applicable to deepfakes, where the "product" is the fake video itself. Regardless, courts have found a likelihood of confusion in false association cases when there was no obvious connection between the plaintiff's fame and the defendant: in *Waits v. Frito-Lay*, for example, where defendant's Doritos commercial featured an allegedly infringing voice-impersonation of Tom Waits, the court affirmed a jury finding of a likelihood of confusion even though there was no connection between Tom Waits' fame and flavored tortilla chips.[254] When courts actually do analyze the relatedness factor, they seem to interpret it broadly, perhaps because public

---

250. Fifty-Six Hope Road Music, Ltd. v. A.V.E.L.A., Inc., 778 F.3d 1059, 1069 (9th Cir. 2015) (applying the *Downing* factors to find a likelihood of confusion as to whether Bob Marley endorsed a sportswear company that used his likeness on its T-shirts).

251. MCCARTHY, *supra* note 74, at § 28:17 ("Applying the first factor in the Ninth Circuit's *Downing* test, a noncelebrity's image would probably have a very low level of recognition among the target audience of millions of persons in the consumer market for defendant's goods or services.").

252. Bondar v. LASplash Cosmetics, No. 12 Civ. 1417(SAS), 2012 WL 6150859, *7 (S.D.N.Y. Dec. 11, 2012) (denying defendant's motion to dismiss plaintiff model's false endorsement claim, even though it was "unlikely the public at large is familiar" with the plaintiff).

253. *See* Electra v. 59 Murray Enterprises, Inc., No. 19-235, 2021 WL 438900, at *18 (2d Cir. Feb. 9, 2021) (reasoning that that the plaintiff—an unknown model—did not have a sufficiently recognized persona to establish a likelihood of confusion). *See also* MCCARTHY, *supra* note 74, at § 28:17 (discussing how the likelihood of confusion test is likely to prevent many non-celebrities from bringing Section 43(a) false endorsement claims).

254. Waits v. Frito-Lay, Inc. 978 F.2d 1093, 1111 (9th Cir. 1992) (affirming jury finding of likelihood of confusion and verdict of false endorsement).

figures have the ability to commercially exploit their fame in a variety of different manners. In *White v. Samsung Elecs. Am., Inc.*, for example, the court found White's fame as a gameshow host was related to the defendant's VCR product, because VCRs can be used to record gameshows.[255] A target of deepfake, such as a political figure, can similarly argue their fame, derived from their public statements and political activities, is related to the defendant's product—a distorted video of such statements and activities.

In addition to the above factors, courts would likely consider whether the false representation in the deepfake is obvious from the context[256] or if the defendant included a disclaimer,[257] the lack of which would potentially weigh against defendants under the fourth factor—"actual confusion"—and the seventh factor—"defendant's intent." In sum, the likelihood of confusion analysis is highly fact-dependent, but deepfakes generally have a high propensity to cause confusion due to how realistic they can appear.

While this Part has outlined the elements of a prima facie case against deepfake creators—use in commerce, in connection with goods or services, false or misleading representation of fact, and likelihood of confusion—noting the difficulties in particular of establishing the "in connection with any goods or services" element, litigants must also be aware of potential First Amendment defenses and the ability to secure judgments against third parties.

C. FIRST AMENDMENT DEFENSE

Deepfake creators are likely to raise a First Amendment defense, arguing their videos are expressive works or parodies entitled to First Amendment protections.[258] This Note argues that if a deepfake does not include disclaimers and is effective at deceiving viewers, the creator is unlikely to have a strong First

---

255. White v. Samsung Elecs. Am., Inc., 971 F.2d 1395, 1400 (9th Cir. 1992).

256. *See* Roberts v. Bliss, 229 F. Supp. 3d 240, 252 (S.D.N.Y. 2017) (granting defendant's motion to dismiss false endorsement claims and reasoning that defendant's ad, which "superimpose[d] graphic images of life-sized appetizers over Plaintiff's entire image," was so "outlandish" that a reasonable viewer would recognize it as a parody of plaintiff's video).

257. *See* Allen v. Nat'l Video, Inc., 610 F. Supp. 612, 628 (S.D.N.Y. 1985) ("The failure of defendant National to include any disclaimer on all but one of the uses of the photograph also supports a finding of, at best, dubious motives.").

258. *See* MCCARTHY, *supra* note 74, at § 28:16 ("The *Rogers* test is a balancing of private and public interests when a mark is used in an expressive work. It is not applicable to "commercial" works such as a traditional advertisement or an infomercial.").

Amendment defense. To determine whether an expressive use of a mark (e.g., a persona) is protected, courts apply the two-part *Rogers* test, which protects a defendant's use unless the alleged use (i) has "no artistic relevance" to the disputed work or, (ii) if there is artistic relevance, the use "explicitly misleads as to the source or the content of the work."[259] Courts interpret the second element, "explicitly misleads," as a stricter version of the likelihood of confusion test, requiring the argument for confusion to be "particularly compelling."[260]

In *Warner Brothers Entertainment v. Global Asylum, Inc.*, for example, the Ninth Circuit affirmed a finding that the defendant's "Age of Hobbits" film, which was about early humans that scientists nicknamed "Hobbits," was explicitly misleading and infringing of plaintiff's "Hobbit" trademark.[261] Particularly disfavorable to the defendant was the court's finding that the defendant took specific efforts to deceive viewers and associate the film with the plaintiff by (i) failing to advertise or otherwise inform potential viewers that the film was about early humans rather than Hobbits from J.R.R. Tolkien's folklore, (ii) releasing the film three days before Warner Brothers released the "real" Hobbit movie, and (iii) failing to correct media coverage that described the film as "a reimagined version of J.R.R. Tolkien's mythical universe."[262] Even assuming a deepfake's use of a plaintiff's persona is artistically relevant to the content of the deepfake, most deepfakes are likely to "explicitly" mislead in a manner analogous to that of the "Age of Hobbits" film. Like the defendants in *Global Asylum*, deepfake creators go out of their way to craft highly realistic videos that are likely to deceive their viewers.

Deepfake creators may argue that even if their videos initially create confusion, the viewer will eventually deduce the fakery. Indeed, in *Cliffs Notes, Inc. v. Bantam Doubleday Dell Pub. Group, Inc.,* where the defendant sold parodic "Spy Notes" books featuring the "distinctive yellow color, black diagonal stripes and black

---

259.   Rogers v. Grimaldi, 875 F.2d 994, 999 (2d Cir. 1989).
260.   Twin Peaks Prods., Inc. v. Publ'ns Intern., Ltd., 996 F.2d 1366, 1379 (2d Cir. 1993). *See also* 6 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 31:144.50 (5th ed. 2021) (discussing the *Rogers* test and collecting cases from different circuits applying it).
261.   Warner Bros. Ent. v. Glob. Asylum, Inc., No. CV 12-9547 PSG (CWx), 2012 WL 6951315, at *17 (C.D. Cal. Dec. 10, 2012), *aff'd sub nom*. Warner Bros. Ent., Inc. v. Glob. Asylum, Inc., 544 F. App'x 683 (9th Cir. 2013).
262.   *Id.* at *13.

lettering of Cliffs Notes," the Second Circuit held there was no likelihood of confusion and therefore the defendant's use could not be explicitly misleading under *Rogers*.[263] The court reasoned that even if consumers were confused by the cover, they would most likely open the books and identify them as parodies before purchasing them.[264] In the same vein, deepfake videos may initially mislead their viewers but, upon being viewed in their entirety, may be obviously fake.

Many deepfakes, however, are distinguishable from the books discussed in *Cliffs Notes*: a deepfake viewer—i.e., an internet user—may not watch enough of a deepfake to identify it as fake, and, more significantly, unlike the Spy Notes books, a deepfake may have zero disclaimers, whether explicit or contextual, that it is fake. Unless the fakery is deducible from the context of the video or there is a disclaimer,[265] the creators of pernicious deepfakes are unlikely to have a strong First Amendment defense under the *Rogers* test.

D. SECONDARY LIABILITY

As discussed *infra* in Part I, prominent websites like Facebook and YouTube have policies prohibiting pernicious deepfakes and have pursued methods of detecting deepfakes uploaded to their sites.[266] The owners of less resourced or less scrutinized "fringe" websites, however, may choose to ignore deepfakes that are posted on their platforms. As many deepfakes are uploaded to the internet by anonymous trolls who are difficult to trace for the purposes of a lawsuit, it may be critical for deepfake targets to be able to sue website owners.[267] Unlike in the case of other causes of action like defamation, discussed *supra* in Part II, false association

---

263.   Cliffs Notes, Inc. v. Bantam Doubleday Dell Publ'n Grp., Inc., 886 F.2d 490, 497 (2d Cir. 1989).

264.   *Id.* at 496.

265.   *See* MCCARTHY, *supra* note 74, at § 31:154 (Judges will generally grant First Amendment defenses and reject infringement claims where "the joke is readily apparent because of the fame of the target mark and/or differences in the overall setting of the parody.").

266.   *See* Bickert, *supra* note 64; *Fake Engagement Policy*, YOUTUBE HELP, https://support.google.com/youtube/answer/3399767?hl=en   [https://perma.cc/5W7M-GG6H].

267.   Before pursuing a claim against a website owner, a plaintiff may seek to subpoena a third-party such as a domain registrar to secure the identity of an anonymous defendant who, for example, owns a website that is posting infringing material. *See, e.g.*, Marketo, Inc. v. Doe, No. 18-CV-06792-JSC, 2018 WL 6046464, at *1 (N.D. Cal. Nov. 19, 2018).

claims against website owners on theories of secondary liability are not foreclosed by Section 230 of the Communications Decency Act.[268] While plaintiffs may additionally pursue a direct claim of false association against website owners, this section discusses the hurdles of pursuing a claim of contributory false association.

1. *Section 230 of the Communications Decency Act*

To establish a contributory false association claim against a website hosting confusing deepfakes uploaded by a third-party user, a plaintiff may need to respond to a challenge that Section 230 of the Communications Decency Act bars such a claim. As will be discussed below, both precedent and historical characterization of the law of false association indicate the claim is not barred.

Section 230(c) of the CDA reads: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[269] This effectively gives websites like Facebook, YouTube, and other social media platforms immunity from causes of action based their publication of material originating from a third party.[270] Such immunity is the reason why Facebook cannot be liable for defamation when a third party user posts a defamatory message on its platform.[271]

The general rule of immunity, however, is accompanied by exceptions in Section 230(e), which stipulates that the statute does not foreclose actions based on, among other things, intellectual property law.[272] Indeed, Section 230(e)(2) states, "Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property,"[273] i.e., the CDA does not immunize websites from secondary liability for intellectual property claims.[274] Courts have interpreted Section 230(e)(2) to allow Lanham Act claims to proceed against website owners, with only a couple of exceptions: some courts—the Ninth and D.C. Circuits—have held that false

---

268. *See* 47 U.S.C. § 230; McCarthy, *supra* note 74, at § 25A:42.50 (collecting cases) ("Since a trademark is clearly a type of "intellectual property," CDA statutory immunity does not shield such claims. All courts agree that a claim under federal law for trademark infringement is an intellectual property claim not precluded by the CDA.").

269. 47 U.S.C. § 230(c).

270. *See* 47 U.S.C. § 230; McCarthy, *supra* note 74, at § 25A:42.50.

271. *See id*; McCarthy, *supra* note 74, at § 25A:42.50.

272. 47 U.S.C. § 230(e)(2).

273. *Id.*

274. McCarthy, supra note 74, at § 25A:42.50.

advertising is not an "intellectual property" claim under Section 230(e)(2) and, therefore, that Section 230 bars contributory false advertising claims against website owners.[275] Similarly, the District Court for the Western District of Washington has held that false designation of origin is not an intellectual property claim and that such a claim is also barred by Section 230.[276] These holdings are non-obvious, however, and the District Court for the Southern District of New York has taken the opposite view, holding that Section 230 bars neither false advertising nor false designation of origin claims.[277]

More importantly, and relevant to this Note, no court has held that Section 230 bars false association claims.[278] Indeed the courts to have addressed the issue, whether in dicta[279] or in their holding,[280] have taken the position that false association claims are not barred by Section 230. Precedent aside, treating the false association claim as arising under intellectual property law for the purposes of Section 230 is consistent with how courts and commentators have historically characterized the claim: "Courts hold that in the context of § 43(a)(1)(A), a human persona or identity is a kind of 'trademark' which is infringed by a false endorsement [i.e., false association]."[281] This is different than false advertising and false designation of origin—the Lanham Act claims that some courts have held do not fall in the intellectual property law exception to Section 230 immunity. Unlike false

---

275. Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1053 (9th Cir. 2019); Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263, 1269 (D.C. Cir. 2019).

276. Corker v. Costco Wholesale Corp., No. C19-0290RSL, 2019 WL 5895430, at *6 (W.D. Wash. Nov. 12, 2019) (barring false designation of origin claim under Section 230).

277. Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 412 (S.D.N.Y. 2001).

278. Of note, in *Corker v. Costco Wholesale Corp.*, the court refers to the plaintiff's claim as "false association" and as "false association of origin," in addition to "false designation of origin," even though the facts pleaded indicate the claim was based on a theory of false designation of origin. No. C19-0290RSL, 2019 WL 5895430, at *4 n.4 (W.D. Wash. Nov. 12, 2019).

279. Stayart v. Yahoo! Inc., 651 F. Supp. 2d 873, 885 (E.D. Wis. 2009), *aff'd*, 623 F.3d 436 (7th Cir. 2010) (stating in dicta, "For example, if Stayart successfully stated a claim for false endorsement under the Lanham Act, Yahoo! would not be immune from liability for those claims because such a claim would probably be considered an intellectual property claim."); Nieman v. Versuslaw, Inc., No. 12-3104, 2012 WL 3201931, at *8 (C.D. Ill. Aug. 3, 2012), *aff'd*, 512 F. App'x 635 (7th Cir. 2013) (in dicta, stating Section 230 would not bar plaintiff's false association claim, if adequately pled).

280. Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 306 (D.N.H. 2008) (holding that the CDA immunized defendant from state law tort claims but allowing false association claim to proceed, unbarred by the CDA).

281. McCarthy, supra note 74, at § 28:15 (citation omitted).

advertising and false designation of origin—which are arguably based solely on false representations themselves rather than on the appropriation of intellectual property rights—false association is premised on the plaintiff's intellectual property right in her persona.[282]   For these reasons, there is strong support for the position that Section 230 does not bar false association claims against website owners.

2. *Contributory Infringement*

Even though the CDA does not grant websites immunity from Lanham Act claims, plaintiffs still must establish contributory infringement in order to hold a website owner accountable, in addition to first establishing direct infringement.[283]   Contributory trademark infringement requires a plaintiff to show the defendant website owner had actual or constructive knowledge of infringement and nonetheless continued to supply its services to the infringer.[284]   In *Louis Vuitton Malletier, S.A. v. Akanoc*, for example, the Ninth Circuit affirmed a jury verdict of contributory infringement where the plaintiff showed that the defendant server operator was aware of infringements on websites it hosted and failed to remove the infringing content in response to at least eighteen Notice of Infringement letters from the plaintiff.[285]   In contrast, in *Tiffany (NJ) Inc. v. eBay, Inc.*, the Second Circuit upheld a finding of no contributory infringement, because Tiffany

---

282.   *See* Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1053–54 (9th Cir. 2019):

> Enigma's Lanham Act claim derives from the statute's false advertising provision. Enigma alleges that Malwarebytes mischaracterized Enigma's most popular software programs in order to divert Enigma's customers to Malwarebytes. These allegations do not relate to or involve trademark rights or any other intellectual property rights. Thus, Enigma's false advertising claim is not a claim "pertaining to intellectual property law" within the meaning of § 230(e)(2). The district court correctly concluded that the intellectual property exception to immunity does not encompass Enigma's Lanham Act claim.

283.   *Id.* at §§ 25:20.50, 25:17 (collecting cases).

284.   *See* Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 110 (2d Cir. 2010) (rejecting a contributory trademark infringement claim by Tiffany against eBay where the plaintiff could not establish whether eBay knew of, and failed to act on, specific infringing uses of Tiffany marks); Louis Vuitton Malletier, S.A. v. Akanoc Sols., Inc., 658 F.3d 936, 942 (9th Cir. 2011) ("To prevail on its claim of contributory trademark infringement, Louis Vuitton had to establish that Appellants continued to supply its services to one who it knew or had reason to know was engaging in trademark infringement.").

285.   *Louis Vuitton Malletier*, 658 F.3d at 940.

did not show eBay had knowledge of specific infringing uses.[286] eBay's general knowledge of counterfeit Tiffany goods and the fact a "significant portion of the 'Tiffany' sterling silver jewelry listed on the eBay website . . . was counterfeit" was not enough to establish contributory infringement.[287]

Although contributory infringement's strict requirement of actual or constructive knowledge is a hurdle, at least the CDA does not immunize websites from contributory false association claims as it does from secondary liability based on other causes of action like defamation.[288] Regardless of the causes of action they ultimately pursue, deepfake targets are most likely to sue only after first pursuing cheaper and more efficient avenues of removing their deepfake from online circulation, such as reporting the videos to the social media sites hosting them. Large, mainstream websites like Facebook and YouTube, as discussed above, have indicated their intentions to protect the public from deepfakes and are therefore more likely to comply with the targets of pernicious deepfakes. Therefore, deepfake targets are most likely to pursue contributory trademark infringement against fringe or less resourced website operators that refuse to comply with Notice of Infringement letters and willfully ignore pernicious and infringing deepfakes uploaded to their websites. As contributory false association claims against website owners are not barred by the CDA, a false association theory may be one of very few options available to deepfake targets who have exhausted non-legal solutions.

CONCLUSION

As the discussion of contributory infringement above indicates, the courtroom is one of many avenues—including third-party detection software and cooperation among social media sites— useful for combatting pernicious deepfakes. This Note has provided an additional tool to the arsenal of those seeking remedies to the harms created by deepfakes. Particularly, this Note has made the case that the law of false association is well-suited to address deepfakes due to its focus on confusion and, crucially, the fact contributory infringement claims are not barred

---

286.   *Tiffany (NJ) Inc.*, 600 F.3d at110.
287.   *Id.* at 98.
288.   *See* MCCARTHY, *supra* note 74, at § 22:4.50.

by the Communications Decency Act. Although false association's standing and "in connection with any goods or services" requirements may pose hurdles to claims against creators of deepfakes unlinked to advertising, this Note has highlighted theories of both requirements under which a plaintiff could arguably proceed.

A false association cause of action against certain deepfake creators may strain existing notions of the Lanham Act. However, deepfake technologies and social media have evolved such that individuals can now profit from creating misleading depictions of others and posting them online—a mischief this Note argues is contemplated by the law of false association. Just as the Lanham Act has adapted to the technological advances of the internet and Photoshop,[289] it may adapt to the rise of deepfakes.

---

289.   *See* Geiger v. C&G of Groton, Inc., 424 F. Supp. 3d 276, 285 (D. Conn. 2019) (holding that the plaintiffs successfully stated a Lanham Act false advertising claim where the defendant altered images of the plaintiffs in order to make it appear that the plaintiffs were affiliated with the defendants' strip clubs).