Protecting Personal Dignity: Advocating for a Federal Right of Publicity Against Pornographic Deepfakes

*Tyler von Denlinger**

"[It] [s]hould be illegal to profit off of somebody's likeness in sex work without consent [whether] its fake or not." – Valkyrae[1]

* J.D. Candidate, Expected May 2024, Chapman University Dale E. Fowler School of Law. B.A. University of California, Berkeley, 2020. Special thanks to Professor Wendy Seiden for guidance and invaluable feedback during the writing process.

1 Rae (@Valkyrae), TWITTER (Jan. 30, 2023, 6:37 PM), https://twitter.com/Valkyrae/status/1620249935529803777?lang=en [https://perma.cc/BT6K-AMLU].

INTRODUCTION

We are currently in a new chapter of the Communication Age. Rapid advancements in information technologies have created new methods in the distribution of digital information. Included in this is the phenomenon of "deepfakes." "Deepfake" describes a "digitally forged image or video of a person that makes them appear to be someone else" through the use of machine-learning algorithms.[2]

Deepfakes use artificial intelligence to create convincing artificial images, audio, and video hoaxes. While some deepfakes are used to make humorous parodies of celebrities and politicians, the most common use of deepfake technology is for sexually explicit media.[3] In 2022, 13,000 pornographic deepfake videos were uploaded to just one well-known deepfake porn site, which accrued a monthly view count of 16 million, with men making up

2 *What is Deepfake Technology?*, TECHSLANG (Sept. 22, 2023), https://www.techslang.com/what-is-deepfake-technology [https://perma.cc/WD5P-MVDB].

3 *See* Kat Tenbarge, *Found Through Google, Bought with Visa and Mastercard: Inside the Deepfake Porn Economy*, NBC NEWS (Mar. 27, 2023, 8:56 AM), https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071 [https://perma.cc/DC9T-SBGT] [hereinafter *Found Through Google*].

84% of the website's audience.[4] In recent years, the demand for deepfake pornography has exploded. In March of 2023, Meta faced backlash after Facebook hosted an ad campaign for a deepfake app where the ad depicted female celebrities in a suggestive manner.[5] In this advertising campaign, the video began by displaying a model in a suggestive position, and then showing the model's body with a female celebrity's face.[6] The barrier to creating these images is nominal. Most platforms only cost around $5 for individuals to create their personal deepfake image, video, or audio.[7] Others, who do not possess the technology, skills, or effort to create their own, can commission others to create pornographic deepfakes, with some offering to create a five-minute video of a "personal girl"—anyone with fewer than two million Instagram followers—for $65.[8]

With the rapid increase in the availability of nonconsensual pornographic deepfakes, everyone—celebrities and average citizens—should be concerned about this epidemic. As evidenced above, no one is safe from pornographic deepfakes, and they may not know they are a victim until their image is trending on X, formerly known as Twitter. While some states have passed deepfake legislation, many do not address pornographic deepfakes, and legislation that does address this topic does not adequately protect victims of deepfake porn.[9] Further, victims who want to punish the website platforms that host deepfake porn are precluded by federal law.[10]

For these reasons, a federal right of publicity must be adopted to protect victims from pornographic deepfakes. A federal right of publicity would give victims the legal standing to sue online platforms that host nonconsensual media and a remedy to remove the deepfakes from these websites.

---

4 *See* Moira Donegan, *Demand for Deepfake Pornography Is Exploding. We Aren't Ready for this Assault on Consent*, THE GUARDIAN (Mar. 13, 2023, 6:16 AM), https://www.theguardian.com/commentisfree/2023/mar/13/deepfake-pornography-explosion [https://perma.cc/9XFG-SYKN]; *see also Mrdeepfakes.com*, SIMILARWEB (Oct. 2023), https://www.similarweb.com/website/mrdeepfakes.com/#overview [https://perma.cc/N7PK-E4ZA].

5 *See* Kat Tenbarge, *Hundreds of Sexual Deepfake Ads Using Emma Watson's Face Ran on Facebook and Instagram in the Last Two Days*, ABC NEWS (Mar. 7, 2023, 12:10 PM), https://www.nbcnews.com/tech/social-media/emma-watson-deep-fake-scarlett-johansson-face-swap-app-rcna73624 [https://perma.cc/3NES-Y4SK].

6 *See id.*

7 *See Found Through Google*, *supra* note 3.

8 *Id.*

9 *See infra* Part I.

10 *See infra* Part II.

A. What are Deepfakes?

Deepfakes are created using digital software, AI machine learning, and face-swapping technology.[11] Creators employ AI technology to combine images to create media depicting statements or actions that did not occur. One example is "face swapping," where the faces between two images or videos are swapped while the rest of the body and environment remains unchanged.[12] For example, researchers trained an AI algorithm using videos of Hillary Clinton, Bernie Sanders, Donald Trump, and Elizabeth Warren.[13] The algorithm was then given videos of comedic impersonators, which then produced videos of them with their faces swapped with their respective political leaders.[14]

Face swapping is only one method to produce a deepfake. Others include speech synthesis and Generative Adversarial Networks ("GAN").[15] Text-to-Speech ("TTS") involves the computer-generated emulation of a person's speech.[16] Earlier versions of TTS had difficulty mimicking a person's cadence;[17] however, the modern technology of "voice cloning" has made it possible to resemble a targeted voice.[18] Similar to face swapping, voice cloning aims to generate an original voice.[19] Voice cloning requires acoustic data sets from an original voice to train a model

---

11 *See* Dave Johnson & Alexander Johnson, *What Are Deepfakes? How Fake AI-Powered Audio and Video Warps Our Perception of Reality*, BUSINESS INSIDER (June 15, 2023, 7:58 AM), https://www.businessinsider.com/guides/tech/what-is-deepfake [https://perma.cc/GK7E-XMWJ].

12 *See generally* Tomasz Walczyna & Zbigniew Piotrowski, *Quick Overview of Face Swap Deep Fakes*, APPLIED SCIS., May 31, 2023, at 1 (detailing the rapid development of facial swapping technology in recent years).

13 *See* Shruti Agarwal et al., *Protecting World Leaders Against Deep Fakes*, COMPUT. VISION FOUND., https://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf [https://perma.cc/38L7-Z33T] (last visited Oct. 9, 2023).

14 *See id.*

15 *See* Betül Çolak, *Legal Issues of Deepfakes*, INST. FOR INTERNET & THE JUST SOC'Y (Jan. 19, 2021), https://www.internetjustsociety.org/legal-issues-of-deepfakes [https:/perma.cc/3GGR-TZDE].

16 *See* Naroa Amezaga & Jeremy Hajek, *Availability of Voice Deepfake Technology and Its Impact for Good and Evil,* THE 23RD ANN. CONF. ON INFO. TECH. EDUC. 23, 24 (2022), https://dl.acm.org/doi/pdf/10.1145/3537674.3554742 [https://perma.cc/B6SL-N6Q7].

17 *See id.*

18 *See* Dave Johnson, *Audio Deepfakes: Can Anyone Tell If They're Fake?*, HOW TO GEEK (Aug. 3, 2020), https://www.howtogeek.com/682865/audio-deepfakes-can-anyone-tell-if-they-are-fake/ [https://perma.cc/KZ5V-QBT7]; *see also* Mohit Saini, *Voice Cloning Using Deep Learning*, MEDIUM (Feb. 6, 2020), https://medium.com/the-research-nest/voice-cloning-using-deep-learning-166f1b8d8595 [https://perma.cc/4JYZ-ME28].

19 *See* Amezaga & Hajek, *supra* note 16, at 24.

capable of generating new audios that sound alike.[20] Recent examples of TTS include voice assistants like Apple's Siri and Amazon's Alexa.[21] Now, there are websites where anyone can create accounts and produce human-quality voice recordings of celebrities and politicians.[22] In February 2023, there was a recent TikTok trend where users would use Voice Lab, a platform created by the AI startup ElevenLabs, to produce fake audio clips of President Joe Biden making provocative statements.[23]

GANs are unique in that this method produces startling, realistic photos and videos of nonexistent individuals.[24] For example, in another research study, photos of nonexistent celebrities were created from thousands of images of real celebrities.[25] These are only some of the methods used to produce deepfakes. As technology continues to develop, so does the advancement of deepfake creation.

B. The Current Rise of Pornographic Deepfakes and Its Impact on Victims

Deepfake technology has been used for decades in generally non-malicious ways. The entertainment industry has widely used such technology in its productions, including dubbing, de-aging actors, and resurrecting deceased actors.[26] The healthcare

---

20 *See id.*

21 *See Conversational AI Examples: How Siri, Alexa & Google Assistant Have Human-Like Conversations*, CFTE (Feb. 11, 2021), https://blog.cfte.education/conversational-ai-examples-how-siri-alexa-google-assistant-have-human-like-conversations/ [htpps://perma.cc/T9VB-Q9EJ].

22 *See* Saini, *supra* note 18 (discussing Lyrebird's services).

23 *See* Miles Klee, *Fake Biden Speeches Are the Hottest Trend in AI Voice Tech*, ROLLING STONES (Feb. 22, 2023), https://www.rollingstone.com/culture/culture-news/joe-biden-voice-fake-ai-speeches-1234683601/ [https://perma.cc/WH8Z-VCK9] ("'I'm from Scranton,' the simulated Biden said. 'What I'm smoking is dirt. So let's get that straight, Jack. Pure brick. Ass. Okay?'").

24 *See, e.g.*, Karras et al., *Progressive Growing of GANs for Improved Quality, Stability, and Variation*, ICLR 1, 18 (2018), https://research.nvidia.com/sites/default/files/pubs/2017-10_Progressive-Growing-of/karras2018iclr-paper.pdf [https://perma.cc/SM6T-4U3Y].

25 *See id.* at 7–8 (looking at Figure 5's images of imaginary celebrities produced using a random number generator from a dataset that included hundreds of low-resolution photos and a GAN to generate these images).

26 *See* Cooper Hood, *How Deepfake Technology Can Change the Movie Industry*, SCREENRANT (Aug. 29, 2021), https://screenrant.com/movies-deepfake-technology-change-hollywood-how/ [https://perma.cc/EEE4-YLKW]; Jeremy Kahn, *Forget Disinformation. It's Hollywood and Madison Avenue Where Deepfakes Are About to Wreak Havoc*, FORTUNE (June 22, 2021, 8:43 AM), https://fortune.com/2021/06/22/deepfakes-tom-cruise-chris-ume-metaphysic-hollywood-madison-avenue-eye-on-ai/ [https://perma.cc/6SCY-4BNQ]; Tamara Kneese, *How Data Can Create Full-On Apparitions of the Dead*, SLATE (Nov. 2, 2020, 6:14

industry has also started using deepfakes to detect tumors.[27] Individuals have also used deepfake technology for personal, non-malicious reasons, including to co-star in their favorite movie[28] or have a TV character apologize for its franchise's controversial series ending.[29]

While some deepfake creation still requires a sophisticated coder and complex machinery, the democratization of the internet and deepfake technology's rapid rate of improvement mean even regular individuals can create manipulated digital content. This is especially true as some commercial applications have begun to offer individuals the ability to face swap content from their phone or home computer.[30] This includes such software programs as the DeepFaceLab program available via GitHub, FaceSwap, or FaceIt.

In 2017, a Reddit user by the username "deepfakes" created the first modern version of the deepfake.[31] On Reddit, the user posted deepfake creations where he swapped the faces of celebrities, including Gal Gadot, Taylor Swift, and Scarlett Johansson, onto the faces of adult video stars.[32] The Reddit user's creations became massively popular, kicking off the modern

PM), https://slate.com/technology/2020/11/robert-kardashian-joaquin-oliver-deepfakes-death.html [https://perma.cc/2DTB-HEUJ].

27 *See* Jackie Snow, *Deepfakes for Good: Why Researchers Are Using AI to Fake Health Data*, FAST CO. (Jul. 22, 2020, 11:44 PM), https://www.fastcompany.com/90240746/deep-fakes-for-good-why-researchers-are-using-ai-for-synthetic-health-data [https://perma.cc/3BAF-T53L].

28 *See* Ryan Gilbey, *A 'Deep Fake' App Will Make Us Film Stars – but Will We Regret Our Narcissism?*, THE GUARDIAN (Sep. 4, 2019, 12:08 PM), https://www.theguard-ian.com/technology/2019/sep/04/a-deep-fake-app-will-make-us-film-stars-but-will-we-re-gret-our-narcissism [https://perma.cc/C6E7-8VSF].

29 *See* Emily Smith, *Watch a 'Deepfake' Jon Snow Apologize for Final Season of 'Game of Thrones*', PAGE SIX (June 16, 2019, 6:03 AM), https://pagesix.com/2019/06/16/watch-a-deepfake-jon-snow-apologize-for-final-season-of-game-of-thrones/ [https://perma.cc/FHH4-6URD].

30 *See* Matt Binder, *Deepfakes Are Getting Easier to Make and the Internet's Just Not Ready*, MASHABLE (Jan. 17, 2020), https://mashable.com/article/deepfake-impersonation-tech-easy-to-make [https://perma.cc/DJ4Q-FXLA]; *see also* Ivan Mehta, *New Deepfake App Pastes Your Face onto GIFs in Seconds*, THE NEXT WEB (Jan. 13, 2020), https://thenextweb.com/artificial-intelligence/2020/01/13/new-deepfake-app-pastes-your-face-onto-gifs-in-seconds/ [https://perma.cc/J8R6-B89L].

31 *See* Ian Sample, *What Are Deepfakes – and How Can You Spot Them?*, THE GUARDIAN (Jan. 13, 2020, 5:00 AM), https://www.theguardian.com/technol-ogy/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [https://perma.cc/YR62-5LYC].

32 *See id.*

deepfake trend. Experts predict that as much as 90% of online content could be synthetically generated within the next few years.[33]

However, as deepfake technology progresses rapidly, these deepfakes present a massive threat to individuals' privacy. There have already been manipulated videos of celebrities spewing hate speech[34] or their images on pornographic websites.[35] In 2019, a study found that 96% of the deepfake videos posted online were pornographic in nature, and 99% of them were of female celebrities mapped on the faces of adult video stars.[36] However, this threat is not exclusive to celebrities. This technology is also targeting many average women. In 2019, a report found that the website messenger Telegram allowed a deepfake bot DeepNude, to share images of virtually undressed women.[37] DeepNude allowed users to upload photos of women and for $50, they would receive a photo of the subject undressed.[38] While the app was eventually taken down, a new investigation indicates that a similar application has already targeted 100,000 young women, and most were unaware this was done to them.[39]

This case is not unique. As deepfake technology has become widespread, it creates more opportunities for individuals to post nonconsensual deepfake porn. Since 2018, there are now dozens of apps and programs to create pornographic deepfakes, with many of these apps offering free memberships or free trials.[40] Anyone now could easily create deepfake porn from their home computer or mobile phone. With this democratization, more and more people have been targeted by pornographic deepfakes. Now, non-

---

33 *See* Shirin Ghaffary, *What Will Stop AI from Flooding the Internet with Fake Images?*, VOX (June 3, 2023), https://www.vox.com/technology/23746060/ai-generative-fake-images-photoshop-google-microsoft-adobe [https://perma.cc/W5NE-PEUG].

34 *See* Klee, *supra* note 23 ("One snippet sounded like actor Emma Watson reading from Hitler's *Mein Kampf.*"); Joseph Cox, *Voices for Abuse*, VICE (Jan. 30, 2023, 10:12 AM) https://www.vice.com/en/article/dy7mww/ai-voice-firm-4chan-celebrity-voices-emma-watson-joe-rogan-elevenlabs [https://perma.cc/YG7L-KMQQ] (mentioning a video where someone saying "trans rights are human rights" is strangled).

35 *See* Rory Cellan-Jones, *Deepfake Videos 'Double in Nine* Months', BBC (Oct. 7, 2019), https://www.bbc.com/news/technology-49961089 [https://perma.cc/4DSB-GFBQ].

36 *See* Sample, *supra* note 31; *see also* Johnson, *supra* note 11.

37 *See* Karen Hao, *A Deepfake Bot Is Being Used to "Undress" Underage Girls*, MIT TECH. REV. (Oct. 20, 2020), https://www.technologyreview.com/2020/10/20/1010789/ai-deepfake-bot-undresses-women-and-underage-girls/ [https://perma.cc/X6GP-ZUVH] (noting that only women were targeted as the technology did not work on men).

38 *See id.*

39 *See id.*

40 *See Found Through Google*, *supra* note 3.

celebrities are more likely to be sexually preyed upon without their knowledge.[41]

Deepfakes also present a new method of executing revenge porn.[42] By allowing individuals greater access to the technology that digitally unclothes primarily women, it gives rejected men the power to punish women through revenge porn, making more women victim of these acts. Revenge porn has a devasting toll on victims. Many have had to remove themselves from the internet altogether—the so-called "silencing effect."[43] Others have had to change their names, and some have tragically taken their own lives.[44] These women's careers and livelihoods have been substantially impacted by deepfake porn campaigns. Even after these images and videos have been removed, there is a constant fear of re-traumatization because, at any moment, these images and videos could resurface and once again ruin their lives. Deepfake pornography presents a real threat to women.[45]

This article will examine the necessity of a federal right of publicity to protect victims from pornographic deepfakes. A federal right of publicity would give victims the legal standing to sue online platforms that host nonconsensual media and a remedy to remove the deepfakes from these websites.

Part I of this Note will address the current federal and state laws and legislation that address deepfakes and grant standing for

---

41 *See* Hao, *supra* note 37; Ministry of Justice & The Rt Hon Dominic Raab MP, *New Laws to Better Protect Victims from Abuse of Intimate Images*, GOV.UK (Nov. 25, 2022), https://www.gov.uk/government/news/new-laws-to-better-protect-victims-from-abuse-of-intimate-images [https://perma.cc/DHT9-SWVH].

42 *See* Sample, *supra* note 31.

43 Sophie Compton, *More and More Women Are Facing the Scary Reality of Deepfakes*, VOGUE (Mar. 16, 2021), https://www.vogue.com/article/scary-reality-of-deepfakes-online-abuse [https://perma.cc/9PP8-RFVK].

44 *See* Karen Hao, *Deepfake Porn Is Ruining Women's Lives. Now the Law May Finally Ban It.*, MIT TECH. REV. (Feb. 12, 2021), https://www.technologyreview.com/2021/02/12/1018222/deep-fake-revenge-porn-coming-ban/ [https://perma.cc/PTE4-ZBG2].

45 *See* Sample, supra note 31 (quoting Danielle Citron, a professor of law at Boston University, saying: "Deepfake technology is being weaponised against women."); *see also* Rory Cellan-Jones, *Deepfake Videos 'Double in Nine Months',* BBC (Oct. 7, 2019) https://www.bbc.com/news/technology-49961089 [https://perma.cc/WD34-V2VH] ("The debate is all about the politics or fraud and a near-term threat, but a lot of people are forgetting that deepfake pornography is a very real, very current phenomenon that is harming a lot of women."); Drew Harwell, *Fake-Porn Videos Are Being Weaponized to Harass and Humiliate Women: 'Everybody Is a Potential Target*', WASHINGTON POST (Dec. 30, 2018, 10:00 AM), https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target/ [https://perma.cc/U4LK-782R] (describing the plight of Ayyub after she was featured in a deepfake without her consent, including rape threats and being doxxed).

victims to sue. This section of the Note will also discuss the limitations of these bills. Many of these laws do not focus on deepfake revenge pornography. The few laws that do only allow victims to seek relief from the creator or poster, who, as stated above, remain anonymous, making it difficult for victims to seek relief and justice. Part II of this Note will discuss a significant federal law that limits victims' standing to sue internet service providers ("ISPs") for deepfake revenge porn, section 230 of the Communications Decency Act ("Section 230"). Section 230 generally immunizes interactive computer services ("ICSs")[46] from failure to moderate claims. Therefore, victims of deepfake pornography would not be able to punish website hosts who host their nonconsensual image and fail to remove it from their website.

Finally, this Note will briefly explain the right of publicity and examine select states that have passed this right, including California. This section will also address how a federal right of publicity would fall under Section 230's intellectual property exception. The intellectual property carve out would grant victims standing to sue website hosts and provide the remedy of an injunction and damages. A federal right of publicity will also resolve ambiguity between the states regarding the definition of deepfakes, who is protected, and the punishment for their creation. This exception will also explain why the statute's definition of pornographic deepfake must be carefully defined to avoid First Amendment challenges.

I. SHORTCOMINGS IN CURRENT DEEPFAKE REGULATIONS: LIMITED PROTECTION FOR PORNOGRAPHIC DEEPFAKES

There seems to be a "technological arms race" between deepfake creation and regulation.[47] As more legislation is passed and media companies refine their detection of the altered content, deepfake creators have repeatedly found ways to circumnavigate these restrictions. Because the tech industry's detection technology has failed to outpace the ingenuity of deepfake creators, much of the legislation passed is toothless as it becomes

46 Section 230 defines interactive computer services as entities that serve multiple users over the Internet, including ICPs and ISPs. *See* 47 U.S.C. § 230(f)(2).

47 *See* Aasha Shaik, *Deepfake Pornography: Beyond Defamation Law*, YALE CYBER LEADERSHIP F. (July 20, 2021), https://www.cyber.forum.yale.edu/blog/2021/7/20/deepfake-pornography-beyond-defamation-law [https://perma.cc/PDF5-EYX5] ("Deepfakes are yet another example of technology growing exponentially faster than our laws, leaving people already at greater risk of harm without legal protection.").

obsolete at the time of its passing. The current deepfake laws fail to address any harm caused by manipulated explicit content.

A. Federal Deepfake Laws Fail to Recognize the Threat of Pornographic Deepfakes

In 2019, the U.S. House Intelligence Committee held hearings exploring the threat posed by deepfakes on U.S. security.[48] By December 2019, President Trump endorsed the federal deepfake legislation as part of the National Defense Authorization Act ("NDAA") for Fiscal Year 2020.[49] The 2020 NDAA ordered (1) a comprehensive report on the foreign weaponization of deepfakes, (2) the executive branch to notify Congress of "foreign deepfake-disinformation activities targeting US elections," and (3) the creation of a "Deepfakes Prize" competition that seeks to encourage the research of deepfake-detection technologies.[50]

The 2021 NDAA built upon its predecessor. Unlike the 2020 NDAA, which was primarily concerned with the foreign weaponization of deepfakes, the 2021 NDAA hinted at Congressional concern with the "rising epidemic of nonconsensual deepfake pornography."[51] The 2021 NDAA directed the Department of Homeland Security ("DHS") to study not just deepfakes' harm to national security but broader dangers, including fraud, harm to vulnerable groups, and violation of civil rights laws.[52]

The 2020 and 2021 NDAAs represent noteworthy initial strides undertaken by the executive branch to comprehensively investigate the landscape of deepfake technology and its associated detection mechanisms. Nevertheless, it is imperative to underscore that these legislative measures do not furnish immediate redress for victims of deepfake pornography. Their primary focus revolves around the exploration and examination of deepfake technology—they are devoid of any provisions for

---

48 *See generally Open Hearing on Deepfakes and A.I., Before the House Permanent Select Comm. On Intelligence,* 116th Cong. (2019), https://www.youtube.com/watch?v=tdLS9MlIWOk.

49 *See* Jason Chipman et al., *First Federal Legislation on Deepfakes Signed into Law*, JDSUPRA (Dec. 24, 2019), https://www.jdsupra.com/legalnews/first-federal-legislation-on-deepfakes-42346/ [https://perma.cc/FKF5-NXBE].

50 *See* National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, 113 Stat. 1198 (2020).

51 Matthew F. Ferraro, *Congress's Deepening Interest in Deepfakes*, THE HILL (Dec. 29, 2020), https://thehill.com/opinion/cybersecurity/531911-congresss-deepening-interest-in-deepfakes/ [https://perma.cc/6LSA-FPFN].

52 *See id.*

regulatory frameworks or recommendations for prosecution. Furthermore, it is worth noting that the 2020 and 2021 NDAA do not explicitly address the specific issue of pornographic deepfakes. While the 2021 NDAA might indirectly encompass pornographic deepfakes within its purview by directing a DHS investigation into potential violations of civil rights laws, the 2021 NDAA remains exclusively committed to investigative efforts.[53] This underscores the perception that, apart from a limited number of recent publications addressing public awareness campaigns centered on pornographic deepfakes, this concern does not currently occupy a prominent position on the federal government's agenda.

Several legislative proposals have sought to impose regulatory measures and penalties on digitally manipulated media. In 2019, and again in 2021, House Representative Yvette D. Clarke introduced the Defending Each and Every Person From False Appearances by Keeping Exploitation Subject to Accountability ("DEEP FAKES Accountability") Act.[54] The primary objective of this legislation was to institute protective provisions and establish legal penalties for infractions related to deepfake creation.[55] Specifically, the DEEP FAKES Accountability Act would have required deepfake creators to put watermarks or identifying labels on their deepfake creations.[56] In addition, the Act aimed to define new criminal offenses associated with the production of deepfakes that failed to adhere to these watermark and disclosure requisites, as well as those involving the alteration of deepfakes to eliminate such disclosures.[57] Noncompliance with these provisions would render deepfake creators subject to criminal liability for a fine, up to five years in prison, or both.[58] However, despite multiple attempts, this bill encountered Senate resistance and has yet to be reintroduced for further consideration.

The Senate's cautious approach may be justified. Establishing legislation contingent upon identifying deepfakes appears

---

53 *See id*.

54 *See* Tiffany Hsu, *As Deepfakes Flourish, Countries Struggle with Response*, THE NEW YORK TIMES (Jan. 22, 2023, 12:39 PM), https://www.nytimes.com/2023/01/22/business/media/deepfake-regulation-difficulty.html [https://perma.cc/4SBH-ZRNJ]; *see also* DEEP FAKES Accountability Act, H.R. 3230, 116th Cong. (2019); DEEP FAKES Accountability Act, H.R. 2395, 117th Cong. (2021).

55 *See* H.R. 3230; H.R. 2395.

56 *See* H.R. 3230 § 1041(a); H.R. 2395 § 1041(a).

57 *See* H.R. 3230 § 1041(f)(1); H.R. 2395 § 1041(f)(1).

58 *See* H.R. 3230 § 1041(f)(1); H.R. 2395 § 1041(f)(1).

premature,[59] considering the absence of robust and reliable deepfake detection technologies.[60] Without a reliable detection method, it is harder to claim that an unflattering image, video, or audio is manipulated. This is especially true for the average citizen. Presently, deepfake targeting is predominantly skewed toward celebrities, who, owing to their extensive public presence, possess a wealth of documented evidence to disprove the authenticity of manipulated content.[61] The comprehensive documentation of a celebrity's life, image, and activities provides them with ample resources to counter any allegations stemming from deepfake misrepresentations. Conversely, refuting a deepfake is a formidable and daunting task for individuals outside the celebrity sphere. Without direct evidence establishing malicious intent, individuals will likely find it difficult to contest the authenticity of deepfake content.

In addition, deepfake federal law has been slow to establish a clear and comprehensive definition of "deepfake" that aligns with the contemporary understanding of deepfake technology within the tech industry. This failure in accurately defining "deepfake" introduces the risk that these legal provisions may become outdated or irrelevant shortly after their enactment.[62] This issue is illustrated in the Ninth Circuit's decision in *Perfect 10, Inc. v. Google, Inc.,* where the Court gave a now outdated explanation of how the internet works.[63] Adopting a more expansive definition of "deepfake" may accommodate for future advancements in the creation of manipulated digital content, thereby mitigating the risk of the law being rendered obsolete as new technological developments emerge. On the other hand, a broad definition of "deepfake" may open the door for bad actors to exploit the term as

---

59 *See* Hsu, *supra* note 54.

60 Even the Deepfake detection technology winner had difficulties determining whether an image was manipulated, with an error rate of 1/3 of the time. *See* Stephen Shankland, *Deepfake Detection Contest Winner Still Guesses Wrong a Third of the Time*, CNET (June 12, 2020, 8:00 AM), https://www.cnet.com/culture/deepfake-detection-contest-winner-still-guesses-wrong-a-third-of-the-time/ [https://perma.cc/QKX3-V47Y]. Another algorithmic detection system was only 65% accurate. *See* Annie Rauwerda, *Are Humans Better Than AI at Detecting Deepfakes? It's Complicated.*, INPUT (Jan. 11, 2022), https://www.inverse.com/input/tech/are-humans-better-than-ai-at-detecting-deepfakes [https://perma.cc/YM2M-GKMN]. *See also* Kahn, *supra* note 26.

61 *See* Sample, *supra* note 31.

62 *See* Julia Griffith, *A Losing Game: The Law Is Struggling to Keep Up with Technology*, J. HIGH TECH. L. (Apr. 12, 2019), https://sites.suffolk.edu/jhtl/2019/04/12/a-losing-game-the-law-is-struggling-to-keep-up-with-technology [https://perma.cc/RG22-4SWN].

63 Perfect 10, Inc. v. Google, Inc., 653 F.3d 976, 978 (9th Cir. 2011).

a pretext to dismiss unfavorable media coverage as "fake news."[64] While this argument has some merit, it underemphasizes the broader positive impacts that more precise and concrete deepfake legislation would deliver. Enacting a federal deepfake law would provide immediate assistance to victims, rather than deferring solutions and waiting for a potentially more technologically literate Congress in the future and when a definitive definition of "deepfake" is agreed upon.

B. State Deepfake Laws Diverge on their Definition of "Deepfake," What Type of Material is Prohibited, and the Punishment

Only a handful of states have introduced and successfully enacted deepfake legislation, including Virginia, New York, and California.[65] These bills differ in their definition of "deepfake" and offer varying degrees of protection to individuals.

1. Virginia's Legislation on Deepfakes Imposes a High Evidentiary Burden on Plaintiffs

In March 2019, Virginia was the first state to enact legislation explicitly addressing the issue of deepfakes.[66] The Virginia legislature passed section 18.2-386.2 of the Virginia Code.[67] The section addresses the "[u]nlawful dissemination or sale of images of another."[68] VCA section 18.2-386.2 criminalizes the distribution of pornographic deepfakes portraying individuals nude or undressed, exposing private parts of the body.[69] The strength of this law lies in its definition of an "individual," which encompasses

---

64 *See* James Vincent, *Why We Need a Better Definition of 'Deepfake'/Let's Not Make Deepfakes the Next Fake News*, THE VERGE (May 22, 2018, 11:53 AM), https://www.theverge.com/2018/5/22/17380306/deepfake-definition-ai-manipulation-fake-news [https://perma.cc/SND2-D46F] ("At one point 'Trump' even says: 'We all know climate change is fake, just like this video.'").

65 *See* Korey Clark, *'Deepfakes' Emerging Issue in the State Legislatures*, LEXISNEXIS: STATE NET (June 4, 2021), https://www.lexisnexis.com/en-us/products/state-net/news/2021/06/04/Deepfakes-Emerging-Issue-in-State-Legislatures.page [https://perma.cc/P7CH-QVPE]. Other states have introduced bills but have failed—Illinois SB 3171 and HB 5321. *See id.* New Jersey also introduced a deepfake pornography bill at the beginning of 2023. *See* Brad Schnure, *Corrado Introduces Legislation Prohibiting Non-Consensual "Deepfake" Pornography*, N.J.'S 40TH LEGIS. DIST., SENATOR KRISTIN CORRADO (Mar. 6, 2023), https://www.senatenj.com/index.php/corrado/corrado-introduces-legislation-prohibiting-non-consensual-deepfake-pornography/59969 [https://perma.cc/52WK-L5BP].

66 *See* Clark, *supra* note 65.

67 *See* VA. CODE ANN. § 18.2-386.2 (2019).

68 *Id.*

69 *Id.*

both public and private figures.[70] In addition, this statute penalizes not only manipulated videos but also still images.[71] Moreover, this law explicitly covers content created with the intent to "coerce, harass, or intimidate" others.[72] This precise delineation of prohibited content helps mitigate future challenges encountered by broader deepfake laws, such as potential First Amendment conflicts and the substantial operational costs imposed on ISPs and content creators.[73]

Section 18.2-386.2 requires specific intent.[74] Under this Virginia law, deepfake creators must post explicit content with the "intent to depict an actual person . . . recognizable . . . by the person's face, likeness, or other distinguishing characteristic" and with the additional "intent to coerce, harass, or intimidate."[75] This intent requirement substantially limits the effectiveness of the legislation, as it necessitates that victims overcome a formidable burden of proof that may, based on the nature of intent crimes, make it difficult to satisfy. In one instance, political publicist Trevor Fitzgibbon sued the whistleblower lawyer Jesselyn Radack for defamation after Radack accused him of rape.[76] In his complaint, Fitzgibbon included partially explicit photos as evidence of the consensual nature of their relationship, and, in turn, Radack claimed Fitzgibbon's disclosure of these photos violated section 18.2-386.2.[77] However, the D.C. Court disagreed and held that Fitzgibbon's testimony failed to establish the intent element required by the Virginia statute.[78] Requiring specific

---

70 *See* § 18.2-386.2(A) ("For purposes of this subsection, 'another person' includes a person whose image was used in creating, adapting, or modifying a videographic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic.").

71 *See* § 18.2-386.2.

72 *Id.*

73 *See* MATTHEW FEENEY, DEEPFAKE LAWS RISK CREATING MORE PROBLEMS THAN THEY SOLVE, 5, 6, 8, 11, (Regul. Transparency Project ed., 2021).

74 *See* § 18.2-386.2.

75 *Id.*; *see also* Abigail Loomis, *Deepfakes and American Law*, DAVIS POL. REV. (Apr. 20, 2022), https://www.davispoliticalreview.com/article/deepfakes-and-american-law [https://perma.cc/HH6A-NWCE].

76 *See* Eugene Volokh, *Limits of "Revenge Porn" Laws*, REASON: THE VOLOKH CONSPIRACY (Jul. 11, 2019), https://reason.com/volokh/2019/07/11/limits-of-revenge-porn-laws/ [https://perma.cc/PA53-SMXH]; Amended Complaint, Radack v. FitzGibbon, No. 3:18-cv-00247-REP (D. Va. Apr. 29, 2018).

77 *See* Complaint, Fitzgibbon v. Radack, No. 3:18-cv-00247-REP (E.D. Va. Apr. 13, 2018); Order at 3, Radack v. Fitzgibbon, No. 3:18-cv-00247-REP (D.C. Super. Ct. Aug. 22, 2018).

78 *See* Order at 3, Radack v. Fitzgibbon, No. 3:18-cv-00247-REP (D.C. Super. Ct. Aug. 22, 2018) ("Respondent [Fitzgibbon] credibly testified that he filed the lawsuit in order to

intent may inadvertently protect malicious individuals, as the evidentiary requirement to establish such intent is difficult to demonstrate.

2. Exemptions in New York's Deepfake Legislation Raise Concerns About Nonconsensual Sexual Deepfake Distribution

In November 2020, New York Governor Andrew Cuomo signed Senate Bill S5959D into law.[79] A portion of this bill amended New York's civil rights laws to include a private right of action for the "unlawful dissemination or publication of a sexually explicit depiction of an individual."[80] The law defines "depicted individual" as any individual who appears, "as a result of digitization, to be giving a performance they did not actually perform," or that was performed but then later altered.[81] Notably, this legal provision defines "digitization" as "to realistically depict" someone undressed, with "computer-generated nude body parts," or engaging in sexual conduct.[82] Under this law, a depicted individual is entitled to pursue various forms of legal relief, including injunctive remedies, compensatory and punitive damages, as well as the recovery of attorney's fees.[83]

The statute includes two exemptions of concern. First, the law grants immunity to law enforcement personnel who disseminate manipulated media within the scope of their official duties, including presentation at trials or other legal proceedings.[84] While the statute is silent in who may view the media at trial, it needlessly broadens the audience for potentially malicious and nonconsensual content.[85] Second, the statute allows for the publication of pornographic deepfakes under specific circumstances, such as when they pertain to matters of "legitimate

clear his name. Respondent did not testify that he intended to publish the photos maliciously or with the 'intent to coerce, harass, or intimidate' Petitioner [Radack]. Petitioner did not testify and did not put forth any evidence of Respondent's malice or intent to 'harass or intimidate.'").

79 Jodi Benassi, *To Die For – New York Recognizes Publicity Rights of Deceased Performers*, IP UPDATE (Dec. 17, 2020), https://www.ipupdate.com/2020/12/to-die-for-new-york-recognizes-publicity-rights-of-deceased-performers/ [https://perma.cc/66CD-PSXR].

80 Matthew F. Ferraro & Louis W. Tompros, *New York's Right to Publicity and Deepfakes LawBreaks New Ground*, COMPUT. & INTERNET LAW., April 2021, at 1–2; N.Y. CIV. RIGHTS LAW § 52-c (McKinney 2021) (as amended by S. 5959D, 2019-2020 Leg., Reg. Sess. (N.Y. 2020)).

81 § 52-c(1)(a).

82 § 52-c(1)(b).

83 § 52-c(5).

84 *See* § 52-c(4)(a)(i).

85 *See* § 52-c.

public concern," possess inherent "political or newsworthy value," or serve as a "commentary, criticism, or disclosure that is otherwise protected by" the New York State Constitution or the First Amendment.[86] However, the statute does not provide clarity regarding the types of situations that fall within this second exemption.[87] Its inclusion ultimately protects the content poster more than the victim.

3. Strategic and Feasible: California's Approach to Combat Deepfakes

In 2019, the California Legislature passed Assembly Bill 602, which established a private right of action that empowers individuals to take legal action against those who generate or disclose another's sexually explicit content to which the depicted individual did not consent or that was created through deepfake technology.[88] This statute allows victims to pursue "injunctive relief and recover reasonable attorney's fees and costs."[89] This law closed the gap between California's existing criminal and civil revenge porn laws, which had previously lacked provisions explicitly addressing digitally manipulated images and videos.[90]

Codified at section 1708.86, California Assembly Bill 602 is unique because it explicitly avoids using the term "deepfake" in its text. Instead, the statute employs the terms "altered depiction," "depicted individual," and "digitization."[91] "Depicted individual" includes "an individual who appears, as a result of digitization, to be giving a performance they did not actually perform" or appears in an altered representation.[92] The statute defines "digitalization" to include: "(A) The nude body parts of another human being as the nude body parts of the depicted individual. (B) Computer-generated nude body parts as the nude body parts of the depicted individual. (C) The depicted individual engaging in sexual conduct in which the depicted individual did not engage."[93]

---

86 *See* § 52-c(4)(a)(ii).

87 *See id.*

88 *See* 2019 Cal. Stat. 491 (A.B. 602) (codified at CAL. CIV. CODE § 1708.86 (West 2022)).

89 *Id.*

90 *See* Douglas E. Mirell & Joshua Geller, *AB 602 and AB 730: Curbing "Deepfakes" in Pornography and Elections*, DAILY J. (Jan. 8, 2020), https://www.dailyjournal.com/articles/355794-ab-602-and-ab-730-curbing-deepfakes-in-pornography-and-elections [https://perma.cc/CAY7-JM6N].

91 CIV. § 1708.86.

92 *Id.*

93 *Id.*

This expansive language makes section 1708.86 of the California Civil Code one of the most inclusive deepfake laws. It extends the private right of action to various forms of digitally altered content, including shallowfakes.[94] Remarkably, this legislation does not incorporate terms related to machine learning or artificial intelligence, thus avoiding a narrow definition that might become outdated in the face of advancements in deepfake technology.[95] Section 1708.86 also references digital "depiction[s]" of individuals generally. This approach protects all individuals rather than exclusively targeting politicians or celebrities, as seen in legislation enacted by other states.[96]

Like section 18.2-386.2 of the Virginia Code, section 1708.86 of the California Civil Code requires an intent to disclose and to harm.[97] As discussed previously, an intent requirement has its limitations, as it imposes a higher evidentiary burden on victims, which may inadvertently shield bad-faith actors. In addition, the statute broadly defines "[c]onsent" as "an agreement written in plain language signed knowingly and voluntarily by the depicted individual."[98] However, there is little explanation for these terms.[99] It is unclear what "plain language" means in the context of a complex legal contract or how a litigant might prove that the defendant was aware of the lack of consent. The section additionally imposes restrictions on injunctive relief by essentially limiting it to actions against the creator alone, excluding any action against the hosting website where the deepfake was posted due to the impracticability of proving knowledge of a lack of consent.[100] This limitation arises from the statute's alignment with Section 230, which shields interactive computer service providers (ICSPs) from content moderation or the failure to moderate its

---

94 *See id.* Shallowfakes are digitally manipulated videos designed "to exploit an individual's cognitive biases which can result in damage to a target person's reputation even if the fake is of a low quality." HENRY AJDER ET AL., THE STATE OF DEEPFAKES: LANDSCAPE, THREATS, AND IMPACT 11 (Deeptrace ed., 2019). Categories of shallowfakes include "missing context," "deceptive editing," and "malicious transformation." *Id.*

95 *See* CIV. § 1708.86.

96 *Compare id.*, *with* 2019 Tex. Sess. Law Serv. Ch. 1339 (S.B. 751) (West) (protecting only those running for office, not the general public). However, the enacted Texas Senate Bill 751, which was codified as Texas Election Code section 255.004(b), was later held unconstitutional. *See Ex parte* Stafford, 667 S.W.3d 517, 532 (Tex. App. 2023), *petition for discretionary review granted* (Aug. 23, 2023).

97 *See* VA. CODE ANN. § 18.2-386.2(A) (2019); CIV. § 1708.86.

98 CIV. § 1708.86(a)(3)(A).

99 *See id.*

100 *See id.*

content adequately.[101] Due to Section 230, under the state statute, if the creator is difficult to find or judgment proof, victims may face challenges in seeking meaningful compensation for the relief of their injuries, especially if the creator or discloser proves elusive or financially insolvent.[102]

These state statutes differ on the scope of digital content they protect against, the definition of sexually explicit material within their purview, and the severity of the penalties. The inconsistencies may make it difficult for victims to assert their claims against those responsible for their exploitation.

II. SECTION 230 LIMITS VICTIMS' ABILITY TO RECOVER UNDER CURRENT STATE DEEPFAKE LAWS

While the aforementioned state deepfake laws provide potential plaintiffs with a private right to action, the majority of these laws necessitate that the potential litigant possesses the identity of the deepfake creator, discloser, or disseminator. Unfortunately, individuals responsible for generating deepfakes often employ various tactics to evade detection, including the use of encrypted browsers and Virtual Private Networks (VPNs).[103] Because of this difficulty in identifying the deepfake creators and disclosers, victims instead turn to the ICSPs that host the manipulated media to recover.[104] However, these victims cannot recover against ICSPs, primarily due to the protective provisions

---

101 *See If Signed by Governor, California Bill AB-602 Will Provide Private Right of Action for Victims of Sexually Explicit 'Deepfakes'*, BAKERHOSTETLER: DATA COUNSEL (Sept. 26, 2019), https://www.bakerdatacounsel.com/blogs/if-signed-by-governor-california-bill-ab-602-will-provide-private-right-of-action-for-victims-of-sexually-explicit-deepfakes/ [https://perma.cc/KPJ4-LMB6] [hereinafter "DATA COUNSEL"] (explaining the California law "is likely preempted by the federal Communications Decency Act, 47 U.S.C. § 230, which protects internet content providers from liability for unlawful content posted by users of its service"). Section 230's shield provision protects ICSPs from being classified as publishers, and therefore, ensures that they are not liable for taking or not taking down content on its platform, whether that content be illegal, defamatory, etc. *See* 47 U.S.C. § 230(c); *see also infra* Section II.B.

102 *See* DATA COUNSEL, *supra* note 101.

103 *See generally* Alexandra Tashman, *"Malicious Deepfakes" - How California's A.B. 730 Tries (and Fails) to Address the Internet's Burgeoning Political Crisis*, 54 LOY. L.A. L. REV. 1391, 1396–97, 1418 (2021); Tiffany Hsu, *As Deepfakes Flourish, Countries Struggle with Response*, N.Y. TIMES (Jan. 22, 2023), https://www.nytimes.com/2023/01/22/business/media/deepfake-regulation-difficulty.html [https://perma.cc/EH3E-3PQB]; Andy Greenberg, *It's About to Get Even Easier to Hide on the Dark Web*, WIRED (Jan. 20, 2017, 7:00 AM), https://www.wired.com/2017/01/get-even-easier-hide-dark-web [https://perma.cc/5TUK-RWV7].

104 *See, e.g.*, Tashman, *supra* note 103, at 1396–97.

outlined in Section 230.[105] This legal framework renders pursuing legal action against ICSPs an untenable option for victims.

A. Recent Internet Case Study Demonstrates Victim's Redress and Remedy Obstacles

On January 26, 2023, during a stream on Twitch, a live streaming video website, the content creator "Atrioc" was caught with a browser tab displaying a website offering explicit deepfake content featuring popular content creators.[106] This website allows visitors to pay to access pornographic deepfakes of (primarily female) well-known Twitch streamers, including Pokimane, Maya Higa, and QTCinderella.[107] Immediately, fans alerted the affected content creators, with some finding out while they were in the middle of their streams.[108] Many of those depicted—including Pokimane, QTCinderella, and Valkyrae—took to the internet to speak out and demand removal of that deepfakes website.[109]

It was not until the controversy hit the mainstream internet that Atrioc addressed the controversy. On January 30, 2023, Atrioc went online on Twitch to apologize.[110] During his apology, Atrioc attempted to provide context by stating that he had only briefly explored the content.[111] Atrioc characterized his behavior

---

105 47 U.S.C. § 230; *see also* Barbara Ortutay, *What You Should Know About Section 230, the Rule that Shaped Today's Internet*, PBS (Feb. 21, 2023, 10:55 AM), https://www.pbs.org/newshour/politics/what-you-should-know-about-section-230-the-rule-that-shaped-todays-internet [https://perma.cc/4DNE-E7AK].

106 *See* Jason Parker, *What Happened to Atrioc? The Entire Streamer Deepfake Debacle Summarized*, SPORTSKEEDA (Sept. 17, 2023, 11:53 AM), https://www.sportskeeda.com/esports/what-happened-atrioc-the-entire-streamer-deepfake-debacle-summarized [https://perma.cc/WVK7-8P7D].

107 *See* Bianca Britton, *They Appeared in Deepfake Porn Videos Without Their Consent. Few Laws Protect Them*., NBC NEWS (Feb. 14, 2023, 12:48 PM), https://www.nbcnews.com/tech/internet/deepfake-twitch-porn-atrioc-qtcinderella-maya-higa-pokimane-rcna69372 [https://perma.cc/Z9SJ-9TJU].

108 *Id.* The British live-streamer "Sweet Anita" was live on Twitch when her viewers notified her about the website and her likeness in the videos. *See id.*

109 *See* Parker, *supra* note 106; Aarnesh Shirvastava, *"I'm Going to F***king Sue You!" - QTCinderella Addresses the Community Following the Streamer Deepfake Controversy*, SPORTSKEEDA (Jan. 31, 2023, 7:38 AM), https://www.sportskeeda.com/esports/news-i-m-going-f-king-sue-you-qtcinderella-addresses-community-following-streamer-deepfake-controversy [https://perma.cc/MDX9-CL23]; Shreyan Mukherjee, *"Should Be Illegal to Profit Off of Somebody's Likeness in S*x Work" - Valkyrae Provides Her Take on the Streamer Deep Fake Controversy*, SPORTSKEEDA (Jan. 31, 2023, 11:54 AM), https://www.sportskeeda.com/esports/news-should-illegal-profit-somebody-s-likeness-s-x-work-valkyrae-provides-take-streamer-deep-fake-controversy [https://perma.cc/5RMR-PW8M].

110 Joshua Robertson, *Streamer Atrioc Apologises After Watching Pokimane Deepfakes*, THEGAMER (Jan. 30, 2023), https://www.thegamer.com/atrioc-pokimane-maya-apology/?newsletter_popup=1 [https://perma.cc/27YL-RW2F].

111 *See id.*

as "morbid curiosity," emphasizing that he just "clicked something" without further thought.[112] However, Atrioc acknowledged that his behavior was "gross" and stated that he was sorry.[113]

On January 31, 2023, Atrioc posted a TwitLonger[114] in which he specifically apologized to Maya and Pokimane.[115] However, some streamers expressed dissatisfaction with the delay in Atrioc's apology and the overall situation.[116] In her livestream on January 31, 2023, QTCinderella addressed the deepfake controversy to shed light on the emotional distress it caused.[117] QTCinderella emphasized that it was deeply problematic that individuals were "able to look at women who are not selling themselves or benefiting off of being seen s[e]xually . . . . If you're able to look at that, you are the problem."[118] QTCinderella then pledged to pursue legal action against the deepfake website.[119]

However, QTCinderella hit a dead-end. Her lawyers informed her that she had no viable case to pursue against the deepfake website, primarily due to the legal protections afforded to ICSPs under both state and federal law, including Section 230.[120] This case shows how women targeted by pornographic deepfakes have few legal options available for recourse. Instead of placing sole accountability on the creators, the platforms that host the nonconsensual media must also share the burden of blame, especially as the deepfake content continues to circulate even after

---

112 *Id.*

113 *Id.*

114 TwitLonger is a website that allows X users to create posts over 140 characters and share these longer messages to X. *See* TWITLONGER, https://www.twitlonger.com/about [https://perma.cc/K469-KYWM] (last visited May 8, 2023).

115 *See* Brandon Ewing (@Atrioc), TWITLONGER (Feb. 1, 2023), https://www.twitlonger.com/show/n_1ss80dv [https://perma.cc/MM6D-SWZR].

116 *See* Parker, *supra* note 106.

117 *See* Shirvastava, *supra* note 109 ("This is what it looks like to feel violated. This is what it looks like to feel taken advantage of. This is what it looks like to see yourself naked against your will. Being spread all over the internet. This is what it looks like.").

118 *Id.*

119 *See id.*

120 *See* Britton, *supra* note 107 ("Every single lawyer I've talked to essentially have come to the conclusion that we don't have a case; there's no way to sue the [website host]."); Nicholas Wilson, *QTCinderella's Deepfake Lawsuit Just Hit a Heartbreaking Wall*, SVG (Feb. 15, 2023, 12:44 PM), https://www.svg.com/1200585/qtcinderellas-deepfake-lawsuit-just-hit-a-heartbreaking-wall/ [https://perma.cc/RXX9-LXRE]; *see also* discussion *infra* Section II.B.

takedown requests have been issued.[121] Potential plaintiffs face substantial legal challenges and require careful legal maneuvering in their attempts to hold ICSPs accountable.

B. Section 230 and Total Immunity of Internet Service Providers

During the 1990s, ICSPs frequently faced legal actions and were held liable for their users' speech.[122] The pattern eventually changed following the pivotal case of *Stratton Oakmont, Inc. v. Prodigy Services Co.*[123] Prodigy was an early online hosting website that hosted a bulletin board called *Money Talk,* which allowed anonymous users to post messages about finance and investments.[124] In October 1994, an anonymous user on *Money Talk* created a post alleging that the securities investment banking firm, Stratton Oakmont and its president had committed fraud in connection with an initial public stock offering.[125] Stratton Oakmont and its president sued Prodigy and the anonymous user for defamation.[126] On the plaintiffs' motion for partial summary judgment, the New York Supreme Court held that Prodigy's representations and policies were sufficient to classify Prodigy as a "publisher" of the user's statements.[127] The court particularly cited the editorial control exercised by Prodigy's Board Leaders in monitoring messages, setting it apart from platforms like CompuServe's, which merely functioned as an "electronic for-profit library."[128]

The introduction of the Communications Decency Act of 1996 ("CDA"), which includes Section 230, was driven by the intention to counteract the precedent set by *Prodigy*.[129] Section 230 recognized the benefits of the internet, including access to educational resources, a forum for political discourse, and

---

121 *See* Britton, *supra* note 107("If you really want to tackle this problem, go upstream . . . That's where all the power is.").

122 *See The Supreme Court's Google Case Has Free Speech on the Line*, FORBES (Feb. 22, 2023, 8:19 AM), https://www.forbes.com/sites/qai/2023/02/22/the-supreme-courts-google-case-has-free-speech-on-the-line/ [https://perma.cc/9ZTD-BYFS].

123 Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *1 (Sup. Ct. May 24, 1995).

124 *See* DMLP Staff, *Stratton Oakmont v. Prodigy*, DIGIT. MEDIA L. PROJECT (Oct. 15, 2007, 10:45 AM), https://www.dmlp.org/threats/stratton-oakmont-v-prodigy [https://perma.cc/TM3U-8MBD].

125 *See id.*

126 *See id.*

127 *Prodigy*, 1995 N.Y. Misc. LEXIS 229, at *1.

128 *Id.* at *8–13 (distinguishing Prodigy from CompuServe).

129 *See* H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.).

opportunities for cultural development and exchange.[130] However, the drafters felt it was unfair to hold ICSPs liable for their good faith efforts to moderate user content.[131] Therefore, Section 230's purpose was "to promote "the continued development of the Internet and other interactive computer services," preserving "the vibrant and competitive free market" for digital services, and maximizing user control over the content they consume.[132] To accomplish this, Congress established that websites would not be designated as "publishers" of the online content they host.[133] Consequently, ICSPs would not be liable for content moderation decisions made in response to material considered by the provider or user as "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."[134]

Section 230's protective shield has fostered an open internet environment, granting users access to a vast array of content.[135] However, it has also enabled online platforms to host problematic content, including misinformation, calls for genocide, and various instances of civil and human rights abuses, all without facing significant consequences.[136] Many of these platforms view the fines imposed as a cost of doing business.[137] Officials have raised concerns about the sustainability of these extensive legal immunities enjoyed by tech platforms and whether there is need for reform.[138]

While Section 230 appears to grant ICSPs almost total immunity, this shield features particular vulnerabilities. There are three common exceptions to Section 230: (1) if the ICSPs

---

130 *See* 47 U.S.C. § 230(a) (1996) (amended 1998, 2018).

131 *See* Emily Stewart, *Ron Wyden Wrote the Law that Built the Internet*, VOX (May 16, 2019, 9:50 AM), https://www.vox.com/recode/2019/5/16/18626779/ron-wyden-section-230-facebook-regulations-neutrality [https://perma.cc/4A76-GVZR].

132 § 230(b).

133 § 230(c)(1).

134 § 230(c)(2).

135 Sixty percent of the world's population was online in 2020; this equals 4.70 billion users worldwide and 480.34 million users in North America alone. Hannah Ritchie et al., *Internet*, OUR WORLD IN DATA, https://ourworldindata.org/internet [https://perma.cc/EL2T-JDGM] (last visited May 13, 2023).

136 *See* Marguerite Reardon, *Section 230: How It Shields Facebook and Why Congress Wants Changes*, CNET (Oct. 6, 2021, 5:00 AM), https://www.cnet.com/news/politics/section-230-how-it-shields-facebook-and-why-congress-wants-changes/ [https://perma.cc/243W-PHCV].

137 *See, e.g.*, David Shepardson, *Facebook to Pay Record $5 Billion U.S. Fine over Privacy; Faces Antitrust Probe*, REUTERS (July 24, 2019, 5:35 AM), https://www.reuters.com/article/us-facebook-ftc/facebook-to-pay-record-5-billion-u-s-fine-over-privacy-faces-antitrust-probe-idUSKCN1UJ1L9 [https://perma.cc/TN2M-DLG7].

138 *See id.*

induced or contributed to the development of the illegal content (i.e., discriminating based on protected characteristics);[139] (2) if the claim does not arise from the ICSPs' publishing or content moderation decisions (i.e., promissory estoppel in a breach of contract claim);[140] or (3) if the ICSPs' content-removal decision was not made in "good faith" (i.e., filtering or blocking content for anticompetitive reasons).[141]

These exceptions likely do not apply to deepfake pornography. Development of illegal content or breach of contract claims rarely align with the circumstances faced by victims of deepfake pornography, although there may be some limited relevance, as exemplified by *Barnes v. Yahoo!, Inc.*[142] Moreover, as *Enigma Software Group USA v. Malwarebytes, Inc.* suggests, Section 230 protects ICSPs when they moderate content considered obscene, lewd, or lascivious, a category under which deepfake pornography invariably falls.[143]

There is one possible avenue for victims of pornographic deepfakes. Section 230 does not shield platforms that violate intellectual property rights.[144]

III. A FEDERAL RIGHT OF PUBLICITY WOULD GRANT VICTIMS THE ABILITY TO SUE AND RECOVERY REMEDIES FROM ICSPS

Congress should adopt a tailored federal right of publicity. This statute should grant individuals intellectual ownership of their name, voice, signature, photograph, and likeness. Additionally, this statute should adopt California's section 1708.86's structure, expressly omitting a specific definition of "deepfake" and embracing an inclusive definition of "digitalization."

---

139 *See* Fair Hous. Council v. Roommates.com, 521 F.3d 1157, 1165 (9th Cir. 2008).

140 *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1107 (9th Cir. 2009). The Ninth Circuit held that despite Yahoo!'s immunity under Section 230, the plaintiff could sue the company for promissory estoppel because it promised to remove the fake profile but did not do so. *See id.*

141 *See* E-Ventures Worldwide, LLC v. Google, Inc., 188 F. Supp. 3d 1265, 1269, 1273, 1277, 1279 (M.D. Fla. 2016) (denying Google's motion to dismiss because E-Ventures provided sufficient evidence to show that Google may have acted anticompetitively, including showing that E-Ventures directly competed with Google's AdWords); *see also* Enigma Software Grp. USA v. Malwarebytes, Inc., 946 F.3d 1040, 1051–52 (9th Cir. 2019) (holding that § 230(c)(2) protects ICSPs moderating obscene or lewd content, not blocking access to content for anticompetitive reasons).

142 *See Barnes*, 570 F.3d at 1107.

143 *See Enigma Software Grp. USA*, 946 F.3d at 1051–52.

144 *See* 47 U.S.C. § 230(d)(2) (1996) (amended 1998, 2018); *see also infra* Part III.

This statute would safeguard individuals against sexually explicit and obscene technological impersonations, which generate revenue for online platforms. Here, the prohibition of digitally altered media must be confined to pornographic deepfakes that meet the *Miller* obscenity framework.[145] By instituting this statute, victims would be able to directly sue and seek remedies against ICSPs for third-party content. Importantly, this approach aims to circumvent the feasibility challenges and First Amendment concerns that the state-level deepfake laws face.

A. What is the Right of Publicity?

The right of publicity is an intellectual property right that protects an individual from the misappropriation of his or her name, likeness, or other indicia of personal identity—such as voice or likeness—for commercial benefit.[146] The right of publicity was first recognized as an economic right in a case concerning the use of baseball players' images on trading cards.[147] In his opinion, Judge Frank articulated that "a man has a right in the publicity value of his photograph . . . [as] many prominent persons . . . would feel sorely deprived if they no longer received money for authorizing advertisement[]."[148] To date, thirty-six states recognize the right of publicity, through statutory law, common law, or both.[149] No federal statute or common law grant this right to individuals.[150] The states that have adopted the right of publicity vary in their treatment of these rights. Differences among these statutes include whether these rights are encompassed within the state's privacy laws, the extent to which

145 *See infra* Part III.C.

146 *Right of Publicity*, INT'L TRADEMARK ASS'N, https://www.inta.org/topics/right-of-publicity/ [https://perma.cc/PR4H-2ZWJ].

147 *See* Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953) ("We think that, in addition to and independent of that right of privacy . . . a man has a right in the publicity value of his photograph . . . [and] to grant the exclusive privilege of publishing his picture, and that such a grant may validly be made 'in gross.'").

148 *Id.*

149 As of 2019, thirty-six states have recognized the right of publicity in some manner, including statutory and common law. *See* RIGHT OF PUBLICITY (ROP) COMM., INT'L TRADEMARK ASS'N, RIGHT OF PUBLICITY STATE OF THE LAW SURVEY (2019), https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/INTA_2019_rop_survey.pdf [https://perma.cc/VAT6-RA4A].

150 However, federal unfair competition laws protect against false endorsement, association, or affiliation. *Right of Publicity*, *supra* note 146.

they endure posthumously, and whether they can be inherited or assigned.[151]

California has one of the most robust right of publicity frameworks, encompassing both statutory and common law protections. California's recognition of the right of publicity first emerged through common law and stands as a distinct and valid claim.[152] To pursue a common law claim, a plaintiff must establish the following: (1) defendant used plaintiff's identity; (2) defendant appropriated plaintiff's name or likeness to defendant's advantage, commercially or otherwise; (3) lack of consent; and (4) resulting injury.[153] California's common law right of publicity is broader than its statutory counterpart. It encompasses claims pertaining to a person's name, likeness, persona, voice, signature, biographical information, sound-alike voice, and overall identity.[154] The common law right of publicity differs from the statute in that it does not mandate the demonstration of a commercial purpose as a prerequisite for legal action. The two claims diverge in terms of post-mortem rights. Under common law, no post-mortem right exists when the deceased individual did not exploit his or her identity during his or her lifetime.[155] This distinction arises from the common law right of publicity's roots in privacy law, and, as such, the cause of action does not survive beyond the death of the individual whose identity was exploited.[156]

Within its right of publicity statute, California extends protection to a person's name, voice, signature, photograph, and likeness against unauthorized commercial use.[157] In determining the scope of "likeness," courts have applied the "readily identifiable" test,[158] concluding that even drawings and robots, if

---

151 *See* Barbara A. Solomon, *Can the Lanham Act Protect Tiger Woods? An Analysis of Whether the Lanham Act is a Proper Substitute for a Federal Right of Publicity*, 94 TRADEMARK REP. 1202, 1202–03 (2004).

152 *See* Eastwood v. Superior Court, 198 Cal. Rptr. 342, 342 (Cal. Ct. App. 1983).

153 *Id.*

154 *See id.*; *see also* Motschenbacher v. R.J. Reynolds Tobacco Co., 498 F.2d 821, 824–27 (9th Cir. 1974) (including protection of persona).

155 *See* Lugosi v. Universal Pictures, 603 P.2d 425, 431 (Cal. 1979).

156 *See* Comedy III Productions, Inc. v. Gary Saderup, Inc., 21 P.3d 797, 797 (Cal. 2001).

157 *See* CAL. CIV. CODE § 3344(a) (Deering 1978).

158 Newcombe v. Adolf Coors Co., 157 F.3d 686, 692 (9th Cir. 1998) (explaining that a person is "readily identifiable" if someone can "reasonably determine that the person depicted…is the same person who is complaining of its unauthorized use").

sufficiently detailed, constitute "likeness" under this statute.[159] To initiate a claim under this statute, a plaintiff must prove the elements of a common law claim,[160] that the defendant "knowingly" used plaintiff's likeness, and that there is a direct link between the alleged use and commercial purpose.[161] The California statute provides statutory damages of $750 or actual damages, whichever is greater, as well as attributable profits.[162]

California also recognizes the statutory post-mortem right of publicity, which lasts for seventy years after an individual's death.[163] Though the post-mortem right of publicity is freely transferable and heritable, whether a plaintiff may enforce those rights statutorily depends on the decedent's domicile at the time of death.[164]

B. A Federal Right of Publicity Would Provide All Victims Equal Standing and Right to Remedies Against ICSPs, Regardless of Jurisdiction

1. Right of Publicity Statutes May Fall Under the Intellectual Property Exemption to Section 230

Section 230(c)(2) immunizes ICSPs from liability when they make good-faith decisions to moderate content that the ICSP or its users find objectionable.[165] However, Section 230(e)(2) introduces a critical exception to this immunity, explicitly stating that "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property."[166] This exception has prompted arguments from plaintiffs contending that a state's right of publicity statute could supersede an ICSP's Section 230

---

159 Newcombe v. Adolf Coors Co., 157 F.3d 686, 692-93 (9th Cir. 1998) (drawing constitutes likeness); *see also* Wendt v. Host Int'l, Inc., 125 F.3d 806, 810 (9th Cir. 1997) (robot constitutes likeness); *but see* White v. Samsung, 971 F.2d 1395, 1397 (9th Cir. 1992) (holding that less detailed robots may fall short of the "likeness" test).

160 *See* Eastwood v. Superior Court, 198 Cal. Rptr. 342, 342 (Cal. Ct. App. 1983).

161 Downing v. Abercrombie & Fitch, 265 F.3d 994, 1001 (9th Cir. 2001).

162 CIV. § 3344(a).

163 *Id.* § 3344.1.

164 *See* Cairns v. Franklin Mint Co., 292 F.3d 1139, 1149 (9th Cir. 2002) (holding that an estate may not file a cause of action under section 3344.1 if the decedent was not domiciled in California at the time of death); Bravado Int'l Grp. Merch. Servs., Inc. v. Gearlaunch, Inc., No. 16-CV-8657-MWF(CWx), 2018 WL 6017035, at *9 (C.D. Cal. Feb. 9, 2018) (interpreting Ninth Circuit precedent to mean that, if the decedent's domicile at the time of death recognizes a statutory post-mortem right of publicity, the estate may bring a claim under section 3344.1).

165 47 U.S.C. § 230(c)(2) (2018 & Supp. 2021).

166 *Id.* § 230(e)(2).

immunity.[167] The intellectual property exception creates an avenue through which victims of pornographic deepfakes may potentially hold ICSPs accountable for content posted by third parties on their platforms and seek remedies for any misconduct on the part of these ICSPs. The Supreme Court has acknowledged the right of publicity as being "closely analogous to the goals of patent and copyright law."[168] Federal courts have also indicated or expressly affirmed that right of publicity statutes convey an intellectual property right within the purview of the exception outlined under Section 230(e)(2).[169]

Section 230(e)'s explicit mention of state law suggests the incorporation of state right of publicity laws.[170] These references to state law suggest that "when Congress wanted to cabin the interpretation of state law, it knew how to do so."[171] Therefore, the text and structure of Section 230(e) indicate that intellectual property laws fall under this exception. Further, while Congress's purpose for enacting Section 230 was to create a "pro-free-market policy," it was not to "erase state intellectual property rights as against internet service providers."[172] Incorporating state intellectual property law, including the right of publicity, into Section 230(e)(2) aligns seamlessly with Congress's overarching goal of promoting a free-market environment.

However, this proposed solution encounters challenges with state right of publicity laws. One significant point of contention is a circuit split regarding the interpretation of Section 230's intellectual property exception. Some circuits, including the Ninth Circuit, do not extend a state's right of publicity into the scope of

---

167 *See, e.g.*, Hepp v. Facebook, 14 F.4th 204, 210 (3d Cir. 2021).

168 Zacchini v. Scripps-Howards Broad. Co., 433 U.S. 562, 573 (1997).

169 *See* Ford Motor Co. v. GreatDomains.com, Inc., No. 00-CV-71544-DT, 2001 WL 1176319, at *1 (E.D. Mich. Sept. 25, 2001) (construing § 230(e)(2) to preclude application of CDA immunity to claims based on the violation of federal trademark laws); Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001) (holding that § 230(e) applies to "any law pertaining to intellectual property," including state right of publicity statutes); Hepp v. Facebook, 14 F.4th 204, 206 (3d Cir. 2021) (holding that § 230(e) allows state right of publicity claims). *But see* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1119 (9th Cir. 2007) (holding § 230(e) applies to federal intellectual property only); Doe v. Friendfinder Network, Inc., No. 07-cv-286-JL, 2008 WL 2001745, at *1 n.1 (D.N.H. May 8, 2008) (noting that § 230 "does not bar the plaintiff's common law right of publicity by virtue of [section 230]'s intellectual property exception").

170 § 230(e)(3) ("Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section.").

171 *Hepp*, 14 F.4th at 211.

172 *Id.*

Section 230's intellectual property exemption.[173] In contrast, other circuits have cast doubt on whether the right of publicity qualifies as an intellectual property right at all.[174] While the Supreme Court has expressly linked the right of publicity to patent and copyright law, some lower courts have ruled differently based on their respective state statutory scheme.[175] For example, a district judge in the Southern District of New York barred a plaintiff's claim against some of the defendant ICSPs, contending that Section 230(e)(2)'s intellectual property exception did not apply to a New York statutory right of publicity claim, as it was construed as a privacy claim rather than an intellectual property claim.[176]

Furthermore, there is the possibility that deepfakes could fall under the "fair use" doctrine, thus not constituting copyright infringement.[177] Fair use serves as a defense in copyright infringement claims, permitting the unlicensed use of copyrighted material in specific contexts.[178] Courts evaluate fair use based on various factors, with a key consideration being the purpose and character of the use.[179] As to purpose and character, courts assess whether the media is "transformative"—if the new media injects

---

173 *See Perfect 10*, 488 F.3d at 1119 (holding section 230(e) applies to federal intellectual property only); *but see Gucci Am.*, 135 F. Supp. 2d at 413.

174 *See* Joshua Dubnow, *Ensuring Innovation As the Internet Matures: Competing Interpretations of the Intellectual Property Exception to the Communications Decency Act Immunity*, 9 NW. J. TECH. & INTELL. PROP. 297, 307 (2010).

175 *See Zacchini*, 433 U.S. at 573; *see also* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 302—03 (D.N.H. 2008); Estate of Presley v. Russen, 513 F. Supp. 1339, 1352–54 (D.N.J. 1981).

176 *See* Ratermann v. Pierre Fabre USA, Inc., No. 22-CV-325 (JMF), 2023 U.S. Dist. LEXIS 8028, at *15 (S.D.N.Y. Jan. 17, 2023) ("[T]he right [of publicity] 'parallels' the common law right of publicity…[b]ut 'the two causes of action' are distinct, and New York does not recognize the common law right of publicity…[i]nstead, 'the "right of publicity" is encompassed under the Civil Rights Law as an *aspect of the right of privacy*.'") (citations omitted). The plaintiff was granted leave to amend her complaint as to her right of publicity claim against two of the defendants; after filing an amended complaint, the District Court of the Southern District of New York dismissed the defendants' new motion to dismiss, allowing the case to continue. *Id.*; Ratterman, v. Pierre Fabre USA, Inc., 2023 WL 7627425, at *1 (S.D.N.Y., Nov. 14, 2023).

177 Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1793 (2019) ("Whether the fake is sufficiently transformed from the original to earn fair use protection is a highly fact-specific inquiry for which a judicial track record does not yet exist.").

178 *See U.S. Copyright Office Fair Use Index*, COPYRIGHT.GOV, https://www.copyright.gov/fair-use/ [https://perma.cc/7F68-RXBW] (last updated Feb. 2023).

179 *See id.* The fair use factors, as outlined by section 107 of the Copyright Act, that courts look at are: "purpose and character of the use," "nature of the copyrighted work," "amount and substantiality of the portion used in relation to the copyrighted work as a whole," and "effect of the use upon the potential market for or value of the copyrighted work." *Id.*

new elements without a "substitute for the original use of the work."[180] The greater the degree of transformation, the higher the likelihood that a court will recognize it as fair use.[181] Some deepfake creators have successfully argued that, despite a victim's ownership rights, their pornographic deepfake qualifies as fair use due to its transformative nature, as it involves altering the original pornographic content to create something new using someone else's likeness.[182] However, this defense may not be available to ICSPs, as they were not the originators of the deepfake media—ICSPs did not transform the media, they only hosted it. Therefore, this defense may not be raised against victims suing ICSPs that merely host the deepfake content.

2. Resolving State Right of Publicity Challenges and Circuit Splits Through a Federal Right of Publicity

The proposed federal right of publicity statute would establish uniform standing and legal remedies for victims nationwide, irrespective of their residence. It would effectively eliminate discrepancies stemming from the varied right of publicity statutes existing across different states. Currently, the nation's right of publicity framework is a patchwork, with thirty-six states recognizing this right through different mechanisms.[183] Some states have codified the right into their statutes, others regard it as freely transferable upon death, and some restrict its applicability to certain category of individuals.[184] Additionally, only a fraction of states have taken steps to address the threat of pornographic deepfakes and protect their citizens against them.[185]

---

180 *Id.*

181 *See id.* ("'[T]ransformative' uses are more likely to be considered fair.").

182 *See* Douglas Harris, *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, 17 DUKE L. & TECH. REV. 99, 109 (2019) ("[P]ublishing" personal deepfakes makes fair use of another's copyrighted images because it is transformative."); Winston Cho, *Does Kendrick Lamar Run Afoul of Copyright Law by Using Deepfakes in "The Heart Part 5"?*, THE HOLLYWOOD REPORTER (May 12, 2022, 1:05 PM), https://www.hollywoodreporter.com/business/digital/does-kendrick-lamar-run-afoul-of-copyright-law-by-using-deepfakes-in-the-heart-part-51235145596/ [https://perma.cc/W3A7-H42B] ("Copyright attorney Alan Friedman . . . says that the deepfakes in the video appear 'highly transformative' and that 'fair use would be a strong defense to a copyright challenge.'"); Tiffany C. Li, *Kim Kardashian vs. Deepfakes*, SLATE (June 18, 2019, 8:34 PM), https://slate.com/technology/2019/06/deepfake-kim-kardashian-copyright-law-fair-use.html [https://perma.cc/Y2TG-LUYY] (analyzing the Kim Kardashian deepfake and concluding the deepfake likely falls under fair use).

183 *See Right of Publicity State of the Law Survey*, INT'L TRADEMARK ASS'N (2019), https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/INTA_2019_rop_survey.pdf [https://perma.cc/7CP2-HL89] (last visited Jan. 30, 2024).

184 *See supra* Part I.

185 *See supra* Part I.

As previously mentioned, these state laws vary significantly in what digital content they cover, the scope of those protected, and the associated penalties. Introducing a single federal statute would bring consistency, extending protection universally and ensuring that all individuals legal have the ability to seek justice and legal remedies for ICSPs' gross negligence and misconduct online.

Additionally, a federal statute would resolve the existing circuit splits pertaining to the interpretation of the right of publicity statutes. By satisfying Section 230's intellectual property exception, a federal right of publicity statute would resolve the ongoing discord regarding the statutory interpretation of Section 230. The Ninth Circuit, for instance, has interpreted that the intellectual property exception to Section 230 applies to federal intellectual property law *only*.[186] Given the absence of any federal statute or case law recognizing a right of publicity within the Ninth Circuit, those types of claims are currently excluded from Section 230's intellectual property exception. This ruling precludes millions of potential plaintiffs in California, Nevada, Washington, and Arizona from piercing Section 230 immunity to hold ICSPs accountable for hosting malicious deepfakes on their platforms. In contrast, the First Circuit (albeit in dicta),[187] the Third Circuit,[188] and the Southern District of New York[189] have expanded the reach of publicity rights to encompass the intellectual property exemption stipulated in Section 230.

Introducing a federal right of publicity statute that explicitly emphasizes its nature as an *intellectual property* right, not a *privacy* right, would resolve the ongoing legal debate within the New York court system. In *Ratermann*, the district court judge determined that the state's right of publicity statute was not covered under Section 230's intellectual property exception, citing established legal precedent.[190] In his opinion, Judge Frank noted that New York courts have continuously construed the state's Civil Rights Laws, encompassing publicity rights, to provide a statutory right to privacy, therefore rendering them ineligible for inclusion within the exception.[191] A federal publicity right would reaffirm

186 *See* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1119 (9th Cir. 2007).

187 *See, e.g.*, Universal Cmty. Sys. v. Lycos, Inc., 478 F.3d 413, 418–20 (1st Cir. 2007).

188 *See* Hepp v. Facebook, 14 F.4th 204, 206 (3d Cir. 2021).

189 *See* Gucci Am., Inc. v. Hall & Assocs, 135 F.Supp.2d 409, 413 (S.D.N.Y. 2001).

190 Ratermann v. Pierre Fabre USA, Inc., No. 22-CV-325 (JMF), 2023 U.S. Dist. LEXIS 8028, at *14 (S.D.N.Y. Jan. 17, 2023).

191 *See id.*

the Supreme Court's classification of the right of publicity as an *intellectual property right* and the substantial body of legal precedent supporting it. Further, a federal statute would allow prospective plaintiffs to sue under this federal law when their state's legal precedent precludes them from pursuing actions against ICSPs under the intellectual property exception.

C. The Federal Right of Publicity Must Prohibit Only Obscene Material to Avoid First Amendment Challenges

Critics of both right of publicity statutes and deepfake laws argue that these laws impede individuals' freedom of speech. Proponents of this view argue that overly broad deepfake legislation would lead to an overregulation of edited content and free speech, potentially leading to constitutional issues, particularly in the case of deepfake laws governing elections.[192] These individuals primarily focus on deepfake bills that regulate speech related to government officials or political candidates and argue that regulated manipulated content, even if false, goes beyond the target of intentionally deceptive content and would suppress political speech.[193] Content moderation concerning politicians or candidates would "not solve the problem of deceptive political videos; it will only result in voter confusion, malicious litigation, and repression of free speech."[194] In addition, these advocates argue election-related deepfake legislation contradicts established First Amendment principles.[195] They emphasize the fact that the Supreme Court has consistently protected false

192 *See* Alex Baiocco, *Political "Deepfake" Laws Threaten Freedom of Expression*, INST. FOR FREE SPEECH (Jan. 5, 2022), https://www.ifs.org/research/political-deepfake-laws-threaten-freedom-of-expression/ [perma.cc/G6BY-A3J4]; *see also* Matthew Feeny, *Deepfake Laws Risk Creating More Problems than They Solve*, THE REGUL. TRANSPARENCY PROJECT OF THE FEDERALIST SOC'Y (Mar. 1, 2021), https://rtp.fedsoc.org/paper/deepfake-laws-risk-creating-more-problems-than-they-solve/ [perma.cc/L4KT-MJ8Y].

193 *See California Becomes the Second State to Restrict Political "Deepfakes"*, FIRST AMEND. WATCH (Oct. 9, 2019), https://firstamendmentwatch.org/california-becomes-the-second-state-to-restrict-political-deepfakes/ [perma.cc/XRL9-VPDX].

194 Kathleen Ronayne, *California Bans 'Deep Fakes' Video, Audio Close to Elections*, ASSOCIATED PRESS (Oct. 4, 2019, 1:35 PM), https://apnews.com/article/4db02da9c1594fd1a199ee0242c39cc2 [perma.cc/H786-HB5Z].

195 *See* Baiocco, *supra* note 192; *see also* Kari Paul, *California Makes 'Deepfake' Videos Illegal, but Law May Be Hard to Enforce*, THE GUARDIAN (Oct. 7, 2019, 6:42 PM), https://www.theguardian.com/us-news/2019/oct/07/california-makes-deepfake-videos-illegal-but-law-may-be-hard-to-enforce [perma.cc/YC3T-JPDQ].

political speech,[196] even when there is misuse by government officials during an election season.[197]

These critics also maintain that this argument extends to other categories of deepfakes. Deepfakes, they argue, fall under the protection of the First Amendment when it safeguards the media.[198] Some scholars have suggested that the right of publicity would permit the unlawful moderation of popular culture and public discourse.[199] Alarmingly, they argue that even pornographic deepfakes could be protected by the First Amendment.[200] For these reasons, they argue that broader legislation regulating speech would be unconstitutional.[201]

If narrowly defined and tailored, a federal right of publicity statute may sidestep potential First Amendment challenges. The federal statute must focus on speech falling outside the scope of constitutionally protected speech.[202] The First Amendment does not protect obscene material.[203] If pornographic deepfakes are categorized within the Supreme Court's definition of "obscenity," then a narrowly tailored regulation targeting their nonconsensual use could withstand the rigorous strict scrutiny standard set forth

196 *See, e.g.*, United States v. Alvarez, 567 U.S. 709, 727 (2012).

197 *See* Feeny, *supra* note 192.

198 *See* Chesney & Citron, *supra* note 177, at 1806; *see also* Russell Spivak, "*Deepfakes": The Newest Way to Commit One of the Oldest Crimes*, 3 GEO. L. TECH. REV. 339, 357–58 (2019).

199 *See* Eugene Volokh, *Freedom of Speech and the Right of Publicity*, 40 HOUS. L. REV. 903, 929–30 (2003) ("[T]here is good reason to think . . . that the right of publicity is unconstitutional as to all noncommercial speech, and perhaps even as to commercial advertising as well."); *see also* Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 CAL. L. REV. 125, 184–96 (1993) (questioning justifications for the right of publicity statutes).

200 *See* United States v. Playboy Ent. Group, Inc., 529 U.S. 803, 812 (2000); *see also* Ashcroft v. Free Speech Coalition, 535 U. S. 234, 239–40 (2002) (upholding First Amendment rights, thereby striking down portions of the federal Child Pornography Prevention Act ("CPPA") of 1996 that banned "virtual child pornography" because the computer-generated images do not classify as obscene or child pornography, categories of unprotected speech).

201 Ashcroft v. ACLU, 542 U.S. 656, 660 (2004) ("[C]ontent-based restrictions on speech [are] presumed invalid . . . the Government bear[s] the burden of showing their constitutionality.") (citations omitted).

202 *See* Rebecca Green, *Counterfeit Campaign Speech*, 70 HASTINGS L.J. 1445, 1486 (2019) (suggesting that a narrowly tailored counterfeited candidate speech—including an intent element and highlight a compelling government purpose—may survive the First Amendment's strict scrutiny test); *see also* Roth v. United States, 354 U.S. 476, 485 (1957) (permitting a criminal obscenity statute a obscenity is not a category of protected speech of the First Amendment).

203 Miller v. California, 413 U.S. 15, 23 (1973) ("This much has been categorically settled by the Court, that obscene material is unprotected by the First Amendment.").

by the Supreme Court in *Reed*.[204] In *Miller*, the Supreme Court outlined factors to determine whether a piece of media was obscene.[205]

The Supreme Court has not directly addressed whether deepfake pornography is obscene, which leaves some uncertainty in this area. However, in *Miller*, the Supreme Court provided examples of obscene content regulation that would not violate free speech, such as "[p]atently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated" or "[p]atently offensive representations or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals."[206] Under this reading, regulation targeting pornographic deepfakes would likely survive a First Amendment challenge if the pornographic deepfake falls within the constraints of obscenity.

Nevertheless, in *Ashcroft v. Free Speech Coalition*, the Supreme Court struck down a bill prohibiting virtual child pornography.[207] In *Ashcroft*, Justice Kennedy, writing for the Court, held that the Child Pornography Prevention Act of 1996 ("CPPA") violated the First Amendment and ignored the *Miller* framework.[208] Justice Kennedy distinguished virtual child pornography and child abuse, remarking that virtual child pornography did not result in actual physical harm to victims.[209] However, there is a distinction between the virtual child pornography depicted in *Ashcroft* and deepfake pornography. Unlike child pornography in *Ashcroft*, deepfake pornography portrays the likeness of individuals.[210] In addition, deepfake pornography does pose actual harm to its victims.[211] While it was

---

204 Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015).

205 *See Miller*, 413 U.S. at 24 (articulating that the trier of fact must consider: "(a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.") (citations omitted).

206 *Id*. at 25.

207 Ashcroft v. Free Speech Coal., 535 U.S. 234 (2002).

208 *Id*. at 246, 255–258 ("The CPPA, however, extends to images that appear to depict a minor engaging in sexually explicit activity without regard to the *Miller* requirements.").

209 *Id*. at 250 (holding that the CPPA overreached by "prohibit[ing] speech that records no crime and creates no victims by its production").

210 *See* Harris, *supra* note 182, at 106 (questioning "whether obscenity lies in the reality of thing deemed obscene or in the depiction of what registers as real").

211 *See, e.g.,* Vasileia Karasavva & Aalia Noorbhai, *The Real Threat of Deepfake Pornography: A Review of Canadian Policy*, 24 CYBERPSYCHOLOGY, BEHAV., & SOC.

not until recently that researchers have begun to study the systematic harm to primarily women due to pornographic deepfakes, the current case studies do give us a good insight. Deepfakes now provide a new instrument for revenge porn, which we have seen ruin careers and reputations, as with former California Representative Katie Hill.[212] Deepfakes have been used to facilitate the exploitation of children[213] and reduce women to sexual objects, leading to great psychological harm.[214]

Given these distinctions, a federal right of publicity statute regulating deepfake pornography in accordance with the *Miller* framework would likely circumvent First Amendment concerns.

CONCLUSION

There has been an exponential rise in the number of pornographic deepfakes since the first modern iteration was posted on Reddit in 2017. Since then, only a few states have passed laws to prohibit or regulate deepfake pornography, but with little success. Many victims of deepfake pornography, the majority featuring women, find themselves without viable legal recourse or remedies, as existing laws often restrict claims to the creators or posters of these deepfakes. This legal impasse is primarily a consequence of Section 230, which curtails the liability of online service providers for content posted by third parties. However, a possible avenue exists through Section 230's intellectual property exemption.

NETWORKING 3 (2021), https://doi.org/10.1089/cyber.2020.0272 [https://perma.cc/R86W-9DNV]; Ashish Jaiman, *Deepfakes Harms & Threat Modeling*, TOWARDS DATA SCI. (Aug. 19, 2020), https://towardsdatascience.com/deepfakes-harms-and-threat-modeling-c09cbe0b7883 [https://perma.cc/8A2U-NUYF]; Rob Toews, *Deepfakes Are Going to Wreak Havoc on Society. We Are Not Prepared*, FORBES (May 25, 2020, 11:54 PM), https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havoc-on-society-we-are-not-prepared/?sh=3fc4fd157494 [https://perma.cc/D8EG-CE8R].

212 *See* Andrew Blankstein, *Former Rep. Katie Hill Sues Ex-Husband, Daily Mail, Redstate.com Over 'Nonconsensual Porn',* NBC (Dec. 22, 2020, 12:30 PM), https://www.nbcnews.com/politics/congress/former-rep-katie-hill-sues-ex-husband-daily-mail-redstate-n1252098 [https://perma.cc/2KBY-AXZ9].

213 In 2021, AI Dungeon, an online game that uses AI-generated text to create choose-your-own-adventure stories from user inputs, depicted scenes that sexually exploited children. *See* Tom Simonite, *It Began as an AI-Fueled Dungeon Game. It Got Much Darker*, WIRED (May 5, 2021, 7:00 AM), https://www.wired.com/story/ai-fueled-dungeon-game-got-much-darker/ [https://perma.cc/H7N7-X2D8]. A moderation system found some user prompts generated "stories depicting sexual encounters involving children." *Id.* Latitude, the creator of AI Dungeon, implemented a more rigid moderation system to root these types of prompts, angering some of its users for limiting their speech. *Id.*

214 Pornographic deepfakes "force individuals into virtual sex" and "can transform rape threats into a terrifying virtual reality." *See* Chesney & Citron, *supra* note 177, at 1773.

The right of publicity is an intellectual property right that protects individuals from the misappropriation of their name, voice, signature, photograph, and likeness. While thirty-six states have introduced some form of the right of publicity, there is an urgent need for a federal law to address this issue comprehensively. Such legislation would harmonize the inconsistencies stemming from various state right of publicity statutes and provide equal legal recourse for all citizens seeking to hold online service platforms accountable. By structuring the statute to specifically target technologically deceptive impersonations that generate revenue for online platforms and by requiring the deepfake pornography to meet the *Miller* obscenity framework, this legal framework ensures that it operates within the bounds of the First Amendment. A federal right of publicity is needed to protect women from the profound harm inflicted by deepfake pornography and to convey a strong message to online platforms about the repercussions of their failure to exercise responsibility and moderation in the face of this malicious content.