

---

---

# A Not-So-Sexy Side of Porn: Examining the Legal Void for Victims of Deepfake Pornography

Sydney Tshimbalanga\*

I.	INTRODUCTION .....	135
II.	BARRIERS OF REGULATING DEEPPAKE PORNOGRAPHY .....	139
	A. <i>Differentiating Revenge Porn Laws</i> .....	140
	B. <i>The First Amendment Defense</i> .....	142
	1. Obscenity .....	142
	C. <i>Section 230</i> .....	144
III.	POSSIBLE REMEDIES .....	146
	A. <i>Intentional Infliction of Emotional Distress</i> .....	147
	B. <i>False Light</i> .....	148
	C. <i>Defamation</i> .....	150
	D. <i>Right of Publicity</i> .....	152
	E. <i>Copyright</i> .....	153
IV.	RISE OF LEGISLATION .....	153
V.	CONCLUSION .....	157

## I. INTRODUCTION

Brandon Ewing, known as “AtrioC” online, was streaming his regularly-scheduled gaming program on Twitch, an online live-streaming service.<sup>1</sup> During his live stream, Ewing accidentally displayed his internet browser, revealing that he had visited a website selling AI-generated pornographic videos of other well-known Twitch streamers.<sup>2</sup> After some

---

\* © 2024 Sydney Tshimbalanga. Managing Editor, Volume 26, *Tulane Journal of Technology and Intellectual Property*, J.D. Candidate 2024, Tulane University Law School; B.S. 2020, Media, Culture, and Communication, New York University, New York, NY. The author wishes to thank her family for their unconditional support, as well as the editors of the *Tulane Journal of Technology and Intellectual Property*.

1. Megan Farokhmanesh, *The Debate on Deepfake Porn Misses the Point*, WIRED (Mar. 1, 2023, 9:00 AM), <https://www.wired.com/story/deepfakes-twitch-streamers-qtccinderella-atric-pokimane/>.

2. *Id.*

of his 318,000 followers who were viewing his live stream quickly reacted to his mistake in the live chat, he issued a tearful apology admitting that he had followed a Pornhub advertisement and bought access to deepfake pornography.<sup>3</sup> A post on X following his apology explained that he was upset about being recognized as a “deepfake porn guy” and promised to remove himself from Twitch and content-creating as a whole.<sup>4</sup> QTCinderella, a streamer and friend of Ewing, was featured in the deepfake publication.<sup>5</sup> She immediately spoke out against Ewing’s actions and expressed her feelings of disgust and violation after seeing her face on fake pornography.<sup>6</sup> Sweet Anita, another streamer and victim of Ewing, explained that she “choose[s] to pass up millions by not going into sex work,” and Ewing’s actions are utter solicitations of her body without consent.<sup>7</sup> While QTCinderella vowed to sue the porn site for spreading its malicious, misleading content to viewers, it now seems impossible to pursue legal action.<sup>8</sup>

The rapid rise of artificial intelligence (AI) has sparked the development of deepfakes, a method that allows individuals to manipulate another person’s image, speech, or actions.<sup>9</sup> Blurring the lines between fact and fiction, deepfake software allows users to synthetically alter footage by digitally modifying a depicted face to appear as someone else.<sup>10</sup> Although this high-tech innovation may sound impressive, the rising popularity of deepfake videos has led to an increased awareness of their potential negative effects on both the victims depicted in such videos and society as a whole.<sup>11</sup>

---

3. Samantha Cole, *‘You Feel So Violated’: Streamer QTCinderella Is Speaking Out Against Deepfake Porn Harassment*, VICE (Feb. 13, 2023, 8:00 AM), <https://www.vice.com/en/article/z34pq3/deepfake-qtcinderella-atric> [https://perma.cc/V8EC-35PT].

4. Brandon Ewing (@Atrioc), X (Feb. 1, 2023, 12:14 AM), <https://x.com/Atrioc/status/1620666941982621696> [https://perma.cc/6RWS-FX5H].

5. Farokhmanesh, *supra* note 1.

6. @QTCinderella, X (Jan. 30, 2023, 1:29 PM), <https://x.com/qtcinderella/status/1620142227250094080?lang=en> [https://perma.cc/EY5V-69J4].

7. @sweetanita, X (Jan. 30, 2023, 1:33 PM), <https://x.com/sweetanita/status/1620143205282103297> [https://perma.cc/N6GU-UG6Y].

8. Lu-Hai Liang, *QTCinderella Finds She Cannot Sue the Creator of Deepfake Site*, THEGAMER (Feb. 15, 2023), <https://www.thegamer.com/qtcinderella-cannot-sue-deepfake-creator/> [https://perma.cc/P6FX-N97R].

9. See Meredith Somers, *Deepfakes, Explained*, MIT SLOAN SCH. OF MGMT. (July 21, 2020), <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained> [https://perma.cc/3E A9-AAVL].

10. *Id.*

11. Abigail Olsen, *The Double-side of Deepfakes: Obstacles and Assets in the Fight Against Child Pornography*, 56 GA. L. REV. 856, 878 (2022).

Well, some deepfakes are harmless. For instance, deepfakes may include parodic-oriented videos of politicians or celebrities that serve as mere entertainment for viewers to laugh at recognizable figures.<sup>12</sup> For example, director Jordan Peele edited his own facial movements on to Barack Obama's face to deliver a comedic interpretation of the former president.<sup>13</sup> While the Obama character is actually Peele himself, the video presented a convincing simulation of a notable face by using machine learning technology.<sup>14</sup> His video is supposed to seem realistic; however, when analyzing its phrasing and context, viewers are able to recognize that it is fake.<sup>15</sup>

Deepfake technology has many positive uses in various industries.<sup>16</sup> Namely, the film industry benefits by digitally editing or dubbing voices in their movies.<sup>17</sup> For example, a malaria awareness campaign featuring David Beckham utilized deepfake technology by altering his voice to make it appear that he was speaking different languages for international viewership.<sup>18</sup> This technology is also used for translating speech for global business purposes when it is necessary to speak to foreign business partners.<sup>19</sup> Additionally, deepfake technology can be used to promote artistic expression.<sup>20</sup> Many children's educational television shows

---

12. See Beatrice Dupuy & Barbary Ortutay, *Deepfake Videos Pose a Threat, But 'Dumbfakes' May Be Worse*, AP NEWS (July 19, 2019, 9:46 AM), <https://apnews.com/article/technology-politics-business-ap-top-news-nancy-pelosi-e810e38894bf4686ad9d0839b6cef93d> [<https://perma.cc/AE2Z-U5U9>].

13. Aja Romano, *Jordan Peele's Simulated Obama PSA is a Double-Edged Warning Against Fake News*, VOX (Apr. 18, 2018, 2:00 PM), <https://www.vox.com/2018/4/18/17252410/jordan-peele-obama-deepfake-buzzfeed> [<https://perma.cc/34Y9-HWW4>].

14. See *id.*

15. *Id.*

16. See Aja Romano, *Deepfakes Are a Real Political Threat. For Now, Though, They're Mainly Used to Degrade Women*, VOX (Oct. 7, 2019, 6:00 PM), <https://www.vox.com/2019/10/7/20902215/deepfakes-usage-youtube-2019-deeptrace-research-report> [<https://perma.cc/T7AR-T9PJ>].

17. Vejay Lalla, Adine Mitrani & Zach Harned, *Artificial Intelligence: Deepfakes in the Entertainment Industry*, WIPO MAG. (June 2022), [https://www.wipo.int/wipo\\_magazine/en/2022/02/article\\_0003.html](https://www.wipo.int/wipo_magazine/en/2022/02/article_0003.html) [<https://perma.cc/ZCP4-RQGY>].

18. Leander Sodji, *How We Made David Beckham Speak 9 Languages*, SYNTHESIA (Oct. 26, 2023), <https://www.synthesia.io/post/david-beckham> [<https://perma.cc/UZJ8-MARX>].

19. Dan Patterson, *Deepfakes for Good? How Synthetic Media is Transforming Businesses*, TECH INFORMED (Oct. 5, 2023), <https://techinformed.com/deepfakes-for-good-how-synthetic-media-is-transforming-business/> [<https://perma.cc/N23E-8E5T>].

20. See Robert Shepherd, *A Real Fake Story*, DEFINITION MAG. (Nov. 23, 2022), <https://definitionmagazine.com/features/a-real-fake-story/> [<https://perma.cc/W7R3-H6LJ>].

feature deepfaked historical figures to provide an engaging, interactive learning method to enrich history courses.<sup>21</sup>

However, while some deepfakes are created without malicious intent, they are often exploited for societal harms.<sup>22</sup> Deepfakes can spark reputational and emotional harms to individuals, with an overwhelming majority targeted towards women, due to the creation of non-consensual deepfake pornography.<sup>23</sup> Pornographic deepfake videos first sparked popularity on Reddit by a user known as Deepfake who regularly posted edited pornography that swapped the faces of celebrities and public figures with pre-made pornographic videos.<sup>24</sup> After gaining popularity, a specialized Reddit page was dedicated exclusively to deepfake content that reached over 90,000 members. Although Reddit eventually banned the page, the rise of deepfake pornography continued to grow rapidly.<sup>25</sup>

As machine-learning technology grew in sophistication, certain software systems provided anyone with basic computer knowledge to create a deepfake.<sup>26</sup> After Reddit removed Deepfake's page due to complaints, another user created a mobile application for smartphones called FakeApp, designed to allow users to create deepfakes, including deepfake pornographic deepfakes, of any individual they desired.<sup>27</sup> Creating a sexualized video of a person, ranging from Hollywood movie stars to a co-worker or ex-girlfriend, became as simple as merely saving their image online and uploading it into the FakeApp program.<sup>28</sup>

With their rise in popularity, deepfakes faced stark criticism as a result of its disparate impact on women.<sup>29</sup> The majority of deepfake

---

21. *Id.*

22. *See* Dupuy & Ortutay, *supra* note 12.

23. Ian Sample, *What are Deepfakes-And How Can You Spot Them?*, GUARDIAN (Jan. 13, 2020, 05:00 PM), <https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them>; *see also* Tatum Hunter, *AI Porn is Easy to Make Now. for Women, That's a Nightmare*, WASH. POST (Feb. 13, 2023, 6:00 AM), <https://www.washingtonpost.com/technology/2023/02/13/ai-porn-deepfakes-women-consent/>.

24. Somers, *supra* note 9.

25. *Id.*

26. *See, e.g.*, Catherine Bernaciak & Dominic A. Ross, *How Easy Is it to Make and Detect a Deepfake?*, CARNEGIE MELON UNIV. SEI BLOG (Mar. 14, 2022), <https://insights.sei.cmu.edu/blog/how-easy-is-it-to-make-and-detect-a-deepfake/> [<https://perma.cc/C8N4-N8RF>].

27. Erik Gerstner, *Face/off: "DeepFake" Face Swaps and Privacy Laws*, 87 DEF. COUNSEL J. 1, 2 (2020).

28. *Id.*

29. *See, e.g.*, Subhiksha Manoj, *Why Mainstream Media Overlooks the Gendered Impacts of Deepfake Tech*, END CYBER ABUSE, <https://endcyberabuse.org/why-mainstream-media-overlooks-the-gendered-impacts-of-deepfake-tech/> [<https://perma.cc/BVP4-VFGL>] (last visited May 31, 2024).

pornography exists within the realm of digitalized sexual assault by contributing to the harmful, gendered effects of the oversexualization of women's bodies and rape culture.<sup>30</sup> Deeptrace, a cybersecurity company, conducted a study and found that ninety-six percent of the total deepfake videos online consisted of non-consensual deepfake pornography. Further, videos on four of the most popular deepfake pornography websites, with over 134 million views, were mostly comprised of female actors and musicians from the entertainment industry.<sup>31</sup> Given that deepfake targets are overwhelmingly female, deepfake pornography inherently exploits and manipulates female sexuality.<sup>32</sup> In turn, this abuse advances misogynistic ideologies and reduces female participation in the digital realm.<sup>33</sup> However, this is just the first step. The use of deepfake pornography could have a further potential impact on the job market for women.<sup>34</sup> For instance, if a recruiter encounters a female candidate with nude images circulating online, they are unlikely to verify its authenticity and are more likely to reject her application altogether.<sup>35</sup>

Due to these concerns, this Comment first examines the current legal barriers that deepfake victims face in their attempt to regulate the creation and distribution of deepfake pornography. Part I explores the barriers posed by current legislation that sweeps over the regulation of deepfakes, such as a creator's First Amendment and Section 230 protections. Part II analyzes the potential legal remedies provided under tort and intellectual property law and how these laws fail to provide adequate protection to victims of deepfake pornography. Lastly, Part III details both the failed and successful attempts by legislatures to enforce laws that prevent the creation and dissemination of deepfake pornography.

## II. BARRIERS OF REGULATING DEEFAKE PORNOGRAPHY

The "deep-fakes problem" has emerged as a significant challenge for courts, victims, and creators, both nationally and globally.<sup>36</sup> This is due to the easy accessibility of such explicit content on widely used

---

30. *Id.*

31. Joseph Cox, *Most Deepfakes Are Used for Creating Non-Consensual Porn, Not Fake News*, VICE (Oct. 7, 2019, 7:47 AM), <https://www.vice.com/en/article/7x57v9/most-deepfakes-are-porn-harassment-not-fake-news> [<https://perma.cc/HNP6-HCPC>].

32. *Id.*

33. *Id.*

34. Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1775 (2019).

35. *See id.*

36. *Id.* at 1758.

platforms like Pornhub and Twitter, which increase its circulation.<sup>37</sup> Although victims may seek legal action as a means of thwarting creators from exploiting their images in non-consensual content, the lack of legislation addressing deepfake pornography combined with protection for creators under the First Amendment and Communications Decency Act (CDA), stand as a colossal barrier to entry.<sup>38</sup>

A. *Differentiating Revenge Porn Laws*

The unauthorized production of deepfake pornography may constitute a form of “revenge porn,” which is considered a type of non-consensual pornographic cybercrime.<sup>39</sup> Today, nearly all fifty states have enacted laws banning individuals from engaging in revenge porn by criminalizing the dissemination of nonconsensual sexually graphic images or videos.<sup>40</sup>

Revenge porn and deepfake pornography are strikingly similar.<sup>41</sup> Like deepfake pornography, revenge porn affects women far more than men and further creates lasting effects for victims, including emotional and psychological harms.<sup>42</sup> Additionally, both involve the nonconsensual distribution of explicit material in violation of an individual’s expectation of privacy.<sup>43</sup> Despite these similarities, it is important to distinguish the crucial differences between revenge porn and deepfake pornography that permit deepfake creators to steer clear of culpability.<sup>44</sup>

While both deepfake pornography and revenge porn involve the non-consensual sharing of sexual content, revenge porn requires that the

---

37. Jack Langa, *Deepfakes, Real Consequences: Crafting Legislation to Combat Threats Posed by Deepfakes*, 101 B.U. L. REV. 761, 766 (2021).

38. *See id.* at 769.

39. James J. Wilkerson, *Revenge Porn: State Laws, Constitutional Challenges, and the Progress of Federal Legislation*, 60 U. LOUISVILLE L. REV. 301, 329 (2022).

40. *Id.* at 302; *see Nonconsensual Distribution of Intimate Images: 48 States + DC + Two Territories Now Have Laws Against Nonconsensual Distribution of Intimate Images*, CYBER CIV. RTS. INITIATIVE, <https://cybercivilrights.org/nonconsensual-distribution-of-intimate-images/> [<https://perma.cc/5DFU-2L2D>] (last visited May 31, 2024). Today, forty-eight states plus Washington D.C., Guam, and Puerto Rico have passed legislation that makes it illegal to distribute a sexually explicit image or video without a person’s consent.

41. Matthew B. Kugler & Carly Pace, *Deepfake Privacy: Attitudes and Regulation*, 116 NW. U. L. REV. 611, 670 (2021).

42. *Id.*

43. *Id.*

44. *Why is Pornography Legal and Prostitution is Not*, HG.ORG, <https://www.hg.org/legal-articles/why-is-pornography-legal-and-prostitution-is-not-31164> [<https://perma.cc/J8J2-C3VZ>] (last visited May 31, 2024) (“Pornography has had a contentious relationship with the law since the middle of the Twentieth Century.”).

distributor has the intention of causing harm or emotional distress to the depicted individual.<sup>45</sup> In contrast, deepfakes are not necessarily created with the intent of harm.<sup>46</sup> Absent pornography, ordinary deepfakes may serve as mere artistic expression, whereas revenge porn is normally deemed a crime.<sup>47</sup> Even when deepfakes contain pornographic material, one can argue that it was created as mere entertainment rather than ill-intent.<sup>48</sup>

Another distinction between deepfake pornography and revenge porn is consent.<sup>49</sup> Revenge porn laws are designed to articulate the differences between the consensual and nonconsensual distribution of intimate images or videos, deeming it illegal if done without a person's consent.<sup>50</sup> On the other hand, deepfakes may be created using images that a person has shared online or obtained without their knowledge or consent.<sup>51</sup> While revenge porn laws focus on the sharing of images or videos without consent, deepfake pornography often involves the creation of an entirely new image or video, absent of the person's knowledge.<sup>52</sup> As a result, the "consent" requirement in deepfake pornography becomes complicated and largely depends on other factors such as whether the person has a reasonable expectation of privacy or whether their image was used with actual intent to deceive.<sup>53</sup>

One of the most important distinctions between revenge porn and deepfake pornography is that the latter does not raise the same privacy concerns as the former simply because the deepfakes do not depict a *real*

---

45. See, e.g., Danielle Citron & Mary Anne Franks, *Evaluating New York's "Revenge Porn" Law: A Missed Opportunity to Protect Sexual Privacy*, HARV. L. REV. BLOG (Mar. 19, 2019), <https://harvardlawreview.org/blog/2019/03/evaluating-new-yorks-revenge-porn-law-a-missed-opportunity-to-protect-sexual-privacy/> [<https://perma.cc/WW4Q-UT2G>] (discussing how New York law only reaches defendants that act with intent to harm their victims).

46. 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/deepfake-revenge-porn-coming-ban/> [<https://perma.cc/N6BP-X652>] ("[I]f the victim can prove the perpetrator's intent to harm, it's possible to use harassment law . . . [b]ut gathering such evidence is often impossible . . .").

47. *Id.*

48. *Id.*

49. Shelby Akerley, *Let's Talk About (Fake) Sex Baby: A Deep Dive into the Distributive Harms of Deepfake Pornography*, 4 ARIZ. L. J. EMERGING TECH. 1, 12 (2021).

50. See Rebecca A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*, 88 FORDHAM L. REV. 887, 922 (2019).

51. *Id.*

52. *Id.*

53. Shannon Reid, *The Deepfake Dilemma: Reconciling Privacy and First Amendment Protections*, 23 U. PA. J. CONST. L. 209, 225 (2021).

person in an event that *actually* occurred.<sup>54</sup> Deepfakes depict an individual's face copied onto a previously created video, therefore the "person" in the video is technically not real.<sup>55</sup> Consequentially, no one's privacy can be at stake if the "person" in the video is not a real person, which in turn, blurs the lines between what is real and what is fake. It then becomes impossible to sue a deepfake creator for exposing explicit content that not only failed to occur, but also did not accurately depict a person's body.<sup>56</sup>

### B. *The First Amendment Defense*

The United States is widely known for its fondness in upholding a citizen's right to free speech. Therefore, anyone who seeks to push for legislation that prohibits the making of deepfake pornography must recognize the possibility of violating a creator's First Amendment right to freedom of speech.<sup>57</sup> While there is a devout interest in allowing individuals to be free to speak on matters within the public domain, these protections may be limited as a means of balancing fundamental rights and preserving a reserved, composed society.<sup>58</sup>

#### 1. Obscenity

Even though all U.S. citizens have the freedom to speak freely, the First Amendment prohibits speech that is considered "obscene."<sup>59</sup> The Supreme Court addressed the issue of whether a state could ban the showing of a film that was seen as obscene in *Jacobellis v. Ohio*.<sup>60</sup> While the justices were divided in their holding, Justice Stewart presented a concurring opinion stating that while he could not define what constitutes obscenity, "he knows it when he sees it."<sup>61</sup> After the 1964 decision, Justice Stewart's phrase was frequently quoted within the context of free speech and obscenity.<sup>62</sup> Although *Jacobellis* did not establish a clear standard for determining obscenity, it was the first time the Court established the

---

54. *Id.*

55. *See id.*

56. *See id.*

57. Akerley, *supra* note 49, at 14.

58. *See id.* at 15.

59. *Miller v. California*, 413 U.S. 15, 36 (1973).

60. 378 U.S. 184 (1964).

61. *Id.* at 197 (Stewart, J., concurring) ("I know it when I see it, and the motion picture involved in this case is not that.").

62. *Id.*; *see also* Peter Lattman, *The Origins of Justice Stewart's "I Know It When I See It,"* WALL ST. J. (Sept. 27, 2007, 5:00 PM), <https://www.wsj.com/articles/BL-LB-4558>.



principle that freedom of expression is protected even when material is viewed as offensive.<sup>63</sup>

The Supreme Court established a more concrete interpretation of obscenity in *Roth v. United States*, holding that it must be “utterly without redeeming social value” to be considered unconstitutional.<sup>64</sup> Concluding that such obscenity is not protected by the First Amendment, the Court further explained that the appropriate test in determining obscenity requires one to establish that an average person viewing the material appeals to prurient interests within contemporary community standards.<sup>65</sup> While the *Roth* test helped clarify and establish a definition of obscenity, it remained difficult for courts to articulate *Roth*’s vague definition.<sup>66</sup>

Sixteen years after the *Roth* decision, the Supreme Court finally articulated a legal definition for obscenity in *Miller v. California*.<sup>67</sup> In *Miller*, the Court designed a three-part test for determining obscenity based on (1) whether the material appeals to prurient interest; (2) whether it depicts sexual conduct in a patently offensive way; and (3) whether it lacks serious literary, artistic, political, or scientific value.<sup>68</sup> If a plaintiff satisfies each prong, her work is considered obscene, diminishing a creator’s First Amendment protection.<sup>69</sup>

While a victim may argue that the *Miller* test bars a deepfake creator from asserting their First Amendment rights, the test may not be effective for evaluating deepfake pornography because the sexual conduct depicted is not based on actual sexual acts or participants.<sup>70</sup> Because deepfakes are manipulated through the use of technology, it is difficult to determine whether the content is patently offensive in light of community standards

---

63. *Jacobellis v. Ohio*, 378 U.S. at 197.

64. *Roth v. United States*, 354 U.S. 476, 497 (1957).

65. *Id.* at 499-500.

66. Shannon Creasy, *Defending Against a Charge of Obscenity in the Internet Age: How Google Searches Can Illuminate Miller’s Contemporary Community Standards*, 26 GA. ST. U. L. REV. 1029, 1032 (2010) (citing KATHLEEN M. SULLIVAN & GERALD GUNTHER, CONSTITUTIONAL LAW 843 (16th ed. 2007) (“The . . . Court’s attempt to define unprotected obscenity in *Roth* spawned a tortuous period of divided rulings . . .”).

67. *See Miller v. California*, 413 U.S. 15 (1973).

68. *See id.* at 24 (“The basic guidelines for the trier of fact must be: (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. If a state obscenity law is thus limited, First Amendment values are adequately protected by ultimate independent appellate review of constitutional claims when necessary.”) (citations omitted).

69. *Id.*

70. Akerley, *supra* note 49, at 18-19.

because it does not correspond to real-world behavior, nulling the second prong.<sup>71</sup> A plaintiff may also find trouble in satisfying the third prong because deepfake pornography is typically created with the sole purpose of satisfying sexual fantasies, meaning that a creator may argue that it constitutes artistic value.<sup>72</sup> Even though deepfake pornography may appeal to prurient interest, satisfying the first prong, that alone is insufficient to deem the material obscene.<sup>73</sup>

### C. Section 230

When a deepfake is uploaded to a website, a question of liability becomes imminent. While the person who creates and posts a deepfake has the potential of facing criminal and civil liability, it is usually difficult to locate and identify the perpetrator due to the anonymity of internet users.<sup>74</sup> Instead of targeting the uploader, a victim may want to seek legal action against the website owner that permitted the uploaded content.<sup>75</sup> However, even though it seems to be a potential loophole, deepfake victims face an additional barrier in doing so after Congress' enactment of Section 230 of the Communication Decency Act.<sup>76</sup>

---

71. See *id.*

72. See, e.g., Jeneanne Orłowski, *Beyond Gratification: The Benefits of Pornography and the Demedicalization of Female Sexuality*, 8 MOD. AM. 53, 54, 64 (2012) (“Proponents for the protection of pornography argue that pornography can be a release of sexual tension that contributes to a decrease in sexual violence . . . . Pornography has given women an outlet to express themselves, a form of literature to educate themselves, and a tool with which to communicate their feelings and lack of fulfillment.”).

73. See *Miller v. California*, 413 U.S. at 24; see also, Bradley J. Shafer, *Sex, Lies, and Videotape: In Critique of the Miller Test of Obscenity*, 70 MICH. B.J. 1038, 1043 (1991) (“Sex and obscenity are simply not synonymous. Yet, even the Supreme Court has noted that the two are separated only by a ‘dim and uncertain line.’ In addition, courts agree that, merely because materials are erotic, sexually explicit, or even ‘hard core,’ those characteristics by themselves do not necessarily render the materials ‘obscene’ or mean that they are anything other than fully protected expression under the First Amendment.”) (footnotes omitted).

74. Lee Rainie, Janna Anderson, & Jonathan Albright, *The Future of Free Speech, Trolls, Anonymity and Fake News Online*, PEW RSCH. CTR. (Mar. 29, 2017), <https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/> [<https://perma.cc/ATB6-YVNP>] (discussing the effect of online anonymity as an enablement of bad behavior).

75. Nicholas O'Donnell, *Have We No Decency? Section 230 and the Liability of Social Media Companies for Deepfake Videos*, 2021 U. ILL. L. REV. 701, 713 (2021) (suggesting that Congress enacts legislation as a means of holding internet companies liable for content posted onto their websites.).

76. 47 U.S.C. § 230(c); see also Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 118 (2009) (“[B]road immunity for operators of abusive websites would eliminate incentives for better behavior by those in the best position to minimize harm.”).

Prior to Section 230, in *Stratton Oakmont v. Prodigy Services Co.*, an investment firm sued Prodigy, a website that allowed users to upload bulletin boards, alleging that it had engaged in fraud.<sup>77</sup> By effectively showing that Prodigy utilized software to scan posts for inappropriate language and had a policy that required employees to mandate and remove offensive posts, the firm was able to argue that it actively participated in the moderation process and acted as a publisher for the website.<sup>78</sup> While the firm succeeded in its claim, the *Prodigy* decision was still questioned by subsequent courts.<sup>79</sup> Under the *Prodigy* view, users may push liability onto online platforms if the site actively played a role in monitoring its content, however, the burden imposed on these websites seemed far too strong.<sup>80</sup> As the Internet became a key force of innovation and economic growth, shielding online platforms from liability was necessary to encourage people to continue their use of online services.<sup>81</sup> Additionally, if websites were to take the blame for all of its users, they could be flooded with legal claims that could result in their financial ruin.<sup>82</sup> Content moderation can also be costly for online platforms as some may not have the means to pay for employees to constantly regulate their websites.<sup>83</sup> After concerns that the emerging Internet would be far too burdened, Congress sought for the enactment of Section 230 of the CDA, granting immunity to websites for the content that users post.<sup>84</sup>

Section 230 of the CDA states that computer services “shall not be treated as the publisher or speaker of any information provided by another

---

77. *Stratton Oakmont, Inc. v. Prodigy Serv. Co.*, No. 31063/94, 1995 WL 323710, at \*1 (N.Y. Sup. Ct. May 24, 1995) (“‘Money Talk’ the board on which the aforementioned statements appeared, is allegedly the leading and most widely read financial computer bulletin board in the United States, where members can post statements regarding stocks, investments and other financial matters.”).

78. *Id.* at \*5-6.

79. *Compare* *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 140 (S.D.N.Y. 1991) (holding that a computer service maintained no more editorial control over the publications it provided than traditional information vendors did, freeing the service from liability because it is unfeasible to expect a company to examine every publication it carried) *with Prodigy*, 1995 WL 323710, at \*1 (holding that the internet service provider was a publisher, thereby holding it liable for content posted by a third party).

80. *See* O’Donnell, *supra* note 75 at 737-38.

81. *Id.*

82. *Id.*

83. Sara Morrison, *Section 230, The Internet Law That’s Under Threat, Explained*, Vox (Feb. 23, 2023, 3:07 PM), <https://www.vox.com/recode/2020/5/28/21273241/section-230-explained-supreme-court-social-media> [<https://perma.cc/6PYF-8STH>] (“Without Section 230’s protections, the internet as we know it today would not exist . . . [M]any websites driven by user-generated content would likely go dark.”).

84. *Id.*

information content provider,” regardless of whether the publisher posts content that may violate the law.<sup>85</sup> Therefore, a plaintiff pursuing legal action would not be able to sue the website. Instead, they would only be able to sue the person who actually published the content to the website.<sup>86</sup> However, this protection has been challenged in the context of deepfake because user anonymity makes it difficult for a victim to identify the person responsible for uploading the content.<sup>87</sup> A smart deepfake creator would not include their actual face and name on a website, which increases the challenge of tracking down the person who distributed the video.<sup>88</sup> Without a perpetrator’s clear identity, there is no way to enforce accountability. Because Section 230 provides such a broad shield of immunity for online platforms, a victim is usually unable to hold a website or publisher liable.<sup>89</sup>

Overall, the legal protections supplied by the First Amendment and Section 230 pose significant barriers for victims seeking legal remedies against the creators and distributors of deepfake pornography.<sup>90</sup> The First Amendment’s free speech protection fairly covers the right to create and disseminate such content, while Section 230 grants immunity to the websites who allow third parties to upload deepfake pornography.<sup>91</sup> The complexities of deepfake technology combined with the lack of consequences creators face limit victims from finding protection from this type of abuse.<sup>92</sup>

### III. POSSIBLE REMEDIES

Although deepfake creators may be given immunity under constitutional and federal law, tort and intellectual property law can potentially provide victims with remedies in their attempt to diminish the exploitation of their image.<sup>93</sup>

---

85. 47 U.S.C. § 230(c)(1).

86. *See id.*

87. *See* Rainie et al., *supra* note 74.

88. *See id.*

89. *See id.*

90. Akerley, *supra* note 49, at 38.

91. *See id.* at 37 (“While third party posters may initiate distribution, it is the continued passive distribution by ISP’s protected by Section 230 immunity that causes the real harm of deepfake pornography.”); *see also*, *Police Dep’t of Chi. v. Mosley*, 408 U.S. 92, 95 (1972) (explaining that “government has no power to restrict expression because of its message, its ideas, its subject matter, or its content,” under the First Amendment).

92. Akerley, *supra* note 49.

93. Molly Mullen, *A New Reality: Deepfake Technology and the World Around Us*, 48 MITCHELL HAMLINE L. REV. 210, 231 (2022).

A. *Intentional Infliction of Emotional Distress*

The most feasible legal recourse for victims of deepfake pornography appears to be through the tort of intentional infliction of emotional distress (IIED).<sup>94</sup> If a victim-plaintiff can demonstrate that “(1) the [p]roducer intended to (2) cause the [v]ictim severe emotional distress (3) by extreme and outrageous conduct and (4) the [v]ictim suffered severe emotional distress as a result of the extreme and outrageous conduct,” they would be eligible to claim compensation under IIED.<sup>95</sup>

Determining what constitutes “extreme and outrageous conduct” depends on a variety of factors including the nature of the conduct, the intent of the perpetrator, and the impact on the victim.<sup>96</sup> Most courts suggest that the conduct must be beyond what a “civilized community” would find tolerable and outside of what “reasonable minds” think is acceptable behavior.<sup>97</sup> For example, the Supreme Court of Connecticut requires an average member of the community to arouse his resentment against the actor’s conduct and lead him to utter, “outrageous!”<sup>98</sup> Therefore, if a deepfake is exceptionally explicit or violent, it may be easier to establish that the conduct was outrageous with intent to cause emotional distress.<sup>99</sup> Additionally, in some cases, if the deepfake creator has a known relationship with the victim such as an ex-boyfriend or ex-husband, the victim could satisfy the “intent” requirement in furtherance of her claim.<sup>100</sup> In these cases, the perpetrator may have intentionally created and distributed the deepfake content with the specific intent to cause emotional distress to the victim.<sup>101</sup>

While IIED claims seem achievable for some victims, most are likely to fall short.<sup>102</sup> At the outset, deepfake content is more likely to be created and distributed anonymously or through fake identities, making it

---

94. See RESTATEMENT (SECOND) OF TORTS § 46 (AM. L. INST. 1965).

95. See Douglas Harris, *Deepfakes: False Pornography is Here and the Law Cannot Protect You*, 17 DUKE L. TECH. REV. 99, 111 (2019) (citing RESTATEMENT (SECOND) OF TORTS § 46 (AM. L. INST. 1965)).

96. See *id.*

97. See, e.g., *Appleton v. Bd. of Educ. of Stonington*, 757 A.2d 1059, 1062 (Conn. 2000).

98. *Id.*

99. See Harris, *supra* note 95, at 111; see also Chesney & Citron, *supra* note 34, at 1794 (arguing that deepfake pornography would qualify as outrageous because it falls “outside the norms of decency.”).

100. See Harris, *supra* note 95, at 112.

101. *Id.*

102. *Id.*

challenging to identify the individual responsible.<sup>103</sup> It is very likely that a creator is unaware that a victim's emotional distress is imminent, therefore the *mens rea* necessary to satisfy the "intent" requirement becomes difficult to prove if a creator simply argues that they did not intend to harm the victim.<sup>104</sup> The second condition for an IIED claim, which requires the victim to experience severe emotional distress, is also difficult to establish because many courts do not consider emotional distress alone as sufficient for liability.<sup>105</sup> Rather, the harassment must be so severe that it results in "mental suffering, mental anguish, mental or nervous shock, or the like."<sup>106</sup> Even though it is possible that a deepfake victim can warrant this reaction, many courts believe that the harassment must be so severe that the victim manifests at least some type of bodily harm rather than mere psychological or reputational harm.<sup>107</sup> In turn, victims of deepfake pornography face a difficult burden in pursuing IIED claims, as the newness of this technology and the complexity of the harm actually caused make it hard to prove the required level of distress and harm.

### B. *False Light*

Given the challenges associated with IIED claims, some victims may opt to pursue a false light claim under right of privacy tort law.<sup>108</sup> False light claims may be relevant in deepfake pornography cases because the use of fabricated images or videos can create a false and misleading impression of the victim, such as engaging in sexual conduct that they never actually participated in.<sup>109</sup> Therefore under the common law, a deepfake creator could potentially face liability for giving "publicity to a matter concerning another that places the other before the public in false light."<sup>110</sup> The Restatement further conditions that the portrayal is highly

---

103. Akerley, *supra* note 49, at 39-40.

104. See Harris, *supra* note 95, at 112 ("IIED claims, thus, appear to be limited to instances where the Producer intentionally sends the deepfake to the Victim or informs her of its circulation on the internet.").

105. See *id.* at 111.

106. See RESTATEMENT (SECOND) OF TORTS § 46 (AM. L. INST. 1965).

107. Adrienne N. Kitchen, *The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment*, 90 CHI.-KENT L. REV. 247, 255, 272 (2015).

108. RESTATEMENT (SECOND) OF TORTS §§ 652B-652D (AM. L. INST. 1977) (The forms are: "Intrusion Upon Seclusion," "Appropriation of Name or Likeness," and "Publicity Given to Private Life").

109. See Harris, *supra* note 95, at 116.

110. RESTATEMENT (SECOND) OF TORTS § 652E (AM. L. INST. 1977).

offensive to a reasonable person and the creator must have had knowledge of his action or acted in reckless disregard when publicizing a victim in false light.<sup>111</sup>

For example, in *Solano v. Playgirl, Inc.*, actor Jose Solano brought a lawsuit against *Playgirl Magazine* after it featured him on the cover with the headline, “Primetime’s Sexy Young Stars Exposed.”<sup>112</sup> Solano claimed that the magazine falsely portrayed that he voluntarily posed for the content, thereby suggesting that he endorsed it when in reality, he was humiliated and embarrassed.<sup>113</sup> The Ninth Circuit concluded that a jury could reasonably find that the cover conveyed a false impression of the actor by eluding that he was willing to pose for the magazine, acknowledging that *Playgirl* published the cover either knowingly or with reckless disregard for its false implications.<sup>114</sup>

Though *Playgirl* highlighted a victory for victims who are portrayed in a false manner, false light claims are subject to additional limitations. The term “publicity” in the Restatement refers to a communication made “to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.”<sup>115</sup> Therefore, determining whether a deepfake creator is subject to liability largely depends on the specific context of the deepfake and the geographic area it encompasses.<sup>116</sup> For example, in California, *Playgirl* held that “the information [must be understood] by one or more persons to whom it was disclosed as stating or implying something highly offensive that would have a tendency to injure [someone’s] reputation.”<sup>117</sup> While California only requires one person to view the publication, the Second Restatement of Torts requires the content to be viewed by the public at large.<sup>118</sup> Deciding what constitutes the “public at large” may be difficult if a deepfake is circulating amongst a small group of friends or has small viewership. Because twenty states follow the Restatement, non-

---

111. *Id.*

112. *Solano v. Playgirl, Inc.*, 292 F.3d 1078, 1080-81 (9th Cir. 2002).

113. *Id.* at 1081 (“He claimed he was humiliated and embarrassed when he learned of the use of his photograph on the cover of *Playgirl* and that he suffered a decline in job offers, invitations to charity events and social contacts with others in the entertainment industry following the publication of the January 1999 issue.”).

114. *Id.* at 1089 (“There is enough disputed evidence to require a jury resolution.”).

115. *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (AM. L. INST. 1977).

116. *See id.*

117. *Solano v. Playgirl*, 292 F.3d at 1082.

118. *See id.*; RESTATEMENT (SECOND) OF TORTS § 652D cmt. a.

recognizable victims who live in these states may find it difficult to prove that a substantial population watched the content.<sup>119</sup>

### C. Defamation

Defamation claims refer to false statements that injure an individual's reputation or cause them to suffer economic or other types of harm.<sup>120</sup> In broad terms, a claim for defamation requires (1) a publication to a third party, (2) with material that identifies the allegedly defamed person, and (3) the material must be defamatory to the ordinary, reasonable person.<sup>121</sup> The law recognizes two subsets of defamation: libel and slander.<sup>122</sup> Libel, the most relevant in the context of deepfakes, targets defamatory expressions by writings, pictures, or any communication embodied in physical form that are injurious to a person's reputation or business, or expose a person to public hatred.<sup>123</sup>

Some argue that defamation law provides an adequate avenue for cases involving deepfake technology. For example, in the pre-Internet case of *Rejent v. Liberation Publications, Inc.*, a male model successfully sued a magazine publisher promoting homosexuality that printed the model's photographs without his consent.<sup>124</sup> The Supreme Court of New York, Appellate Division for the First Department held that a photo that falsely portrays an individual posing for explicit images is defamatory *per se*.<sup>125</sup>

While precedent has barred creators from publishing falsified images in certain cases, defamation laws are often construed narrowly.<sup>126</sup> To prove defamation, an image or video must purport to be true as a means of misleading the public.<sup>127</sup> As a consequence, deepfake creators can easily avoid liability by simply posting the word "fake" in the title of their content. Additionally, viewers are often aware that deepfake content is not real.<sup>128</sup> For example, if a video features a classmate or prominent

---

119. Harris, *supra* note 95, at 117.

120. See Akerley, *supra* note 49, at 41.

121. RESTATEMENT (SECOND) OF TORTS § 559 (AM. L. INST. 1977).

122. *Id.* at § 568.

123. *Id.*

124. *Rejent v. Liberation Publ'ns*, 611 N.Y.S.2d 866, 867 (N.Y. App. Div. 1994).

125. *Id.*

126. See, e.g., *State v. Turner*, 864 N.W.2d 204 (Minn. Ct. App. 2015) (arguing that a Minnesota criminal defamation statute could be upheld by using a narrowing construction).

127. See *Rejent*, 611 N.Y.S.2d at 867.

128. See Danielle Keats Citron, *Sexual Privacy*, 128 YALE L. J. 1870, 1921 (2019).



celebrity that has never been known to participate in pornographic content, it is likely that a viewer knows of its falsity.<sup>129</sup>

A key factor for holding a creator liable for defamation is proving the identity of the victim.<sup>130</sup> For example, a celebrity-plaintiff in a defamation suit has a more stringent standard of proving a defendant acted with actual malice, while a private citizen must show mere negligence.<sup>131</sup> This standard often blurs the lines when determining whether a plaintiff-victim has a valid defamation claim.<sup>132</sup> For instance, in *Dameron v. Washington Magazine*, the district court for the District of Columbia recognized “involuntary public figure” status, which refers to someone involved in an event of societal importance.<sup>133</sup> There, an air traffic controller at the time of a major plane crash brought a libel action against a magazine publisher that placed the air controller at blame for the accident.<sup>134</sup> The court held that the air controller was an involuntary public figure for the limited purpose of the plane crash, therefore subject to the same standard as any public figure.<sup>135</sup> Under the broadened *Dameron* lens, if a victim is considered an “involuntary celebrity,” she would have to show that a creator acted with actual malice, a more stringent standard than if she were considered a private individual.<sup>136</sup> A similar barrier is placed for false light claims.<sup>137</sup> In *Time, Inc. v. Hill*, the Supreme Court added the actual malice requirement from defamation law to false light tort cases involving “matters of public interest.”<sup>138</sup> While a later case reversed the *Hill* decision by holding that “actual malice” only applies to

---

129. See generally Patrick Hough, *The Social Costs of Pornography*, THE WITHERSPOON INST. (Mar. 23, 2010), <https://www.thepublicdiscourse.com/2010/03/1215/> [<https://perma.cc/4GDN-ZSCY>] (“With the arrival of the internet age, people of all ages, genders, and classes now have an almost unlimited access to pornographic content that is tailored to every acquired taste and fantasy. The material’s immediate accessibility is enhanced by seemingly endless development of more vivid, more realistic digital media . . .”).

130. See Delfino, *supra* note 50, at 901 (“The same distortion and anonymity issues involved in deepfakes’ creation make it difficult to naturally fit these doctored videos into existing laws, which does not settle the question of who should be held responsible for acts involving deepfakes.”).

131. Gary Bugh, *Public Figures and Officials*, FREE SPEECH CTR. AT MIDDLE TENN. STATE UNIV., <https://mtsu.edu/first-amendment/article/1010/public-figures-and-officials> [<https://perma.cc/N3DU-2MHX>] (last visited May 31, 2024).

132. *Id.*

133. See *Dameron v. Wash. Mag., Inc.*, 575 F. Supp. 1575, 1578 (D.D.C. 1983).

134. *Id.* at 1576.

135. See *id.* at 1578.

136. See Derigan Silver & Loryn Rumsey, *Going Viral: Limited-Purpose Public Figures, Involuntary Public Figures, and Viral Media Content*, 27 COMM. L. & POL’Y 49, 52 (2022).

137. *Dameron*, 575 F. Supp. at 1577.

138. 385 U.S. 374, 388 (1967).

plaintiffs who are public figures, most states continue to follow the original *Hill* approach, leaving the correct standard up in the air.<sup>139</sup>

*D. Right of Publicity*

The right of publicity, an intellectual property right, contains an additional barrier for non-celebrity victims of deepfake pornography.<sup>140</sup> While any person is able to file a false light, defamation, and IIED claim, right of publicity violations are designed to protect only the names and likenesses of celebrities.<sup>141</sup> Vanna White, the well-known Wheel of Fortune host, was awarded damages in the Ninth Circuit after a Samsung commercial featured a robot that dressed like her and mimicked her actions.<sup>142</sup> In *White v. Samsung Electronics America, Inc.*, the court held that because Samsung attempted to monetize from the use of White's image in its advertisement, the company had a commercial interest in utilizing her identity, therefore invading her name and likeness.<sup>143</sup>

Although *White* recognized the effects that look-alike use has against a celebrity-victim, a deepfake creator may find loopholes under the current law. First, the right of publicity only protects the *commercial* use of one's identity, however in many cases, deepfake creators are not seeking commercial gain or profit.<sup>144</sup> Instead, creators often make deepfakes for entertainment or self-gratification purposes, barring them from liability under the law.<sup>145</sup> Additionally, the average citizen does not have the social status to be able that their likeness is being appropriated. The *White* court explained that the right of publicity theory is vested in the right of a celebrity as an identifiable figure who has an interest in protecting the "unauthorized commercial exploitation" of their identity.<sup>146</sup> Therefore, the ruling suggests that an everyday citizen is not subject to commercial exploitation because they may not be identifiable or generate commercial value.<sup>147</sup> Consequently, this poses a significant obstacle for

---

139. See Bugh, *supra* note 131.

140. See Russell Spivak, "Deepfakes": *The Newest Way to Commit One of the Oldest Crimes*, 3 GEO. L. TECH. REV. 339, 383-86 (2019).

141. See *id.*

142. *White v. Samsung Elecs. Am., Inc.*, 971 F.2d 1395, 1396 (9th Cir. 1992).

143. *Id.*

144. See *id.* at 1398; see also, Spivak, *supra* note 140, at 381 ("The tort of wrongful appropriation requires that the defendant appropriate the plaintiff's likeness to his own use or benefit.' Usually, such use or benefit is attributed to a commercial or financial benefit." (quoting *Ault v. Hustler Mag., Inc.*, 860 F.2d 877, 883 (9th Cir. 1988))).

145. See Akerley, *supra* note 49 at 41.

146. *White*, 971 F.2d at 1398.

147. See *id.*

ordinary individuals affected by deepfakes since it is improbable that their content will accrue any commercial value.

*E. Copyright*

If a deepfake includes copyrighted material, the creator of the revised deepfake video may be liable for copyright infringement.<sup>148</sup> Although copyright infringement may hold the deepfake creator accountable for infringing on the original creators work, it still gives little help for the victim of the subsequent production.<sup>149</sup> A victim may assert that the creator infringed on her own personal copyright because anyone who creates an image holds its copyright; however, winning this claim is difficult.<sup>150</sup> The fair use doctrine promotes freedom of expression by permitting the unlicensed use of copyright-protected work in certain circumstances.<sup>151</sup> If the new work is considered “transformative,” meaning it injects a new element without substituting the original work, it is likely that the new work is free from infringing on the copyrighted material.<sup>152</sup> Therefore, when a victim asserts that she holds a copyright in her photos that are later used in an unauthorized deepfake, because the creator modified her image by editing it onto a different work, a different, transformative work is created, and the fair use doctrine is applicable.<sup>153</sup>

IV. RISE OF LEGISLATION

In December 2018, then-Senator Ben Sasse (R-NE) introduced the Malicious Deep Fake Prohibition Act of 2018 (MDFPA), a bill attempting to criminalize the creation and distribution of deepfakes.<sup>154</sup> The MDFPA would prohibit the creation of deepfakes, acknowledging that its distribution would facilitate criminal or tortious conduct under federal, state, or local law.<sup>155</sup> The bill applied to creators who intended to partake in illegal activity, such as fraud, by posting the deepfake to a platform, and it would further criminalize the platform if it were aware that it

---

148. See O’Donnell, *supra* note 75, at 712.

149. See Harris, *supra* note 95, at 107.

150. *Id.*

151. See U.S. CONST. art. I., § 8, cl. 8. (“The Congress shall have Power . . . [t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries[.]”).

152. Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994).

153. See Harris, *supra* note 95, at 109.

154. See Malicious Deep Fake Prohibition Act of 2018, S. 3805, 115th Cong. (2018).

155. *Id.*; see also Kaveh Waddell, *Lawmakers Plunge into “Deepfake” War*, AXIOS (Jan. 31, 2019), <https://www.axios.com/2019/01/31/deepfake-laws>.

participated in deepfake distribution.<sup>156</sup> If violated, a creator may be subject to a fine and two years' imprisonment, or up to ten years imprisonment if the deepfake could potentially disrupt the government or an election.<sup>157</sup> While the Senator's bill was short-lived and ultimately rejected, Sasse's attempt to criminalize the distribution of deepfakes was viewed as an initial stepping point for federal legislation to be enacted for victims in the future.<sup>158</sup>

On December 20, 2019, Congress passed the National Defense Authorization Act (NDAA) for Fiscal Year 2020, which addressed the issue of deepfakes relating to national security violations.<sup>159</sup> Section 5709, titled "Report on Deepfake Technology, Foreign Weaponization of Deepfakes, And Related Notifications," required the Director of National Intelligence (DNI) to provide reports to congressional intelligence committees about the potential impact that deepfakes had on national security and the use of deepfakes by foreign governments to spread disinformation.<sup>160</sup> The NDAA served as a solution for effectively combating deepfakes on a federal level and demonstrated that deepfakes were a true concern for the country.<sup>161</sup> While the NDAA provided a stepping stone for acknowledging the harm of deepfakes, it may be a mere glimmer of hope for victims who are affected on an individual level since the Act focused solely on issues of national security.

While many suggest utilizing the existing legal remedies to bring civil and criminal actions to combat deepfakes on an individual level, lawmakers did not consider the rise of technology when drafting such legislation. Due to the unpredictable nature of AI technology, rather than relying on current legislation, few states have passed laws holding deepfake creators liable for their work.<sup>162</sup> Initially, state-enacted deepfake laws were enacted as a means of preventing political tampering, such as election interference.<sup>163</sup> For example, in 2019, Texas passed SB 751 which barred deepfake creators from fabricating a deceptive as an attempt

---

156. *Id.*

157. *See* S. 3805.

158. *See* O'Donnell, *supra* note 75 at 711.

159. *See* Matthew F. Ferraro, *Congress's deepening interest in deepfakes*, THE HILL (Dec. 29, 2020, 12:00 PM), <https://thehill.com/opinion/cybersecurity/531911-congresss-deepening-interest-in-deepfakes/>.

160. 50 U.S.C. § 5709.

161. *See id.*

162. *See* Langa, *supra* note 37, at 774.

163. *See* DEEP FAKES Accountability Act, H.R. 3230, 116th Cong. (2019) (The DEEP FAKES Accountability Act seeks to protect against the harms enforced by nonconsensual pornography to foreign interference in elections).

to fabricate elections.<sup>164</sup> Similarly, California passed the Elections: Deceptive Audio or Visual Media Act which bans creators for producing “an image . . . or video recording of a candidate’s appearance, speech or conduct that has been intentionally manipulated” in a manner that falsely appears authentic.<sup>165</sup> While the language of the statutes provides a method of criminalizing deepfakes, they only apply to political candidates running for elected office, leaving everyday individuals subject to harm.<sup>166</sup>

However, several states have enacted new regulations to prevent the negative impacts of deepfakes in other circumstances. Rather than merely applying directly to election interference, these laws serve as a guide to create broader legislation for everyday individuals. For example, Virginia passed a bill to combat deepfake pornography.<sup>167</sup> The statute prohibits the unauthorized distribution or sale of any video-graphic or still images that depict a “person who is totally nude, or in a state of undress.”<sup>168</sup>

Similarly in 2019, AB-602 passed in California, creating a civil private right of action for victims of deepfake pornography.<sup>169</sup> Instead of explicitly using the term “deepfake,” the statute refers to “altered depiction,” “depicted individual,” and “digitization.”<sup>170</sup> The statute suggests that “depicted individual” refers to an individual who, because of digitization, appears to be giving a performance they did not actually perform or to be performing in an altered depiction.<sup>171</sup> Therefore, it is safe to assume that deepfakes fall within these protected terms.<sup>172</sup>

More recently, on May 5, 2023, Rep. Joseph Morelle (D-NY) reintroduced the Preventing Deepfakes of Intimate Images Act aimed at prohibiting the nonconsensual dissemination of digitally manipulated

---

164. S.B. 751, 86th LEG. REG. SESS. (Tex. 2019) (enacted).

165. CAL. ELEC. CODE § 20010 (West 2023).

166. *Id.* at § 20010(a) (“[A] person . . . or other entity shall not, within 60 days of an election at which a candidate for elective office will appear on the ballot, distribute, with actual malice, materially deceptive audio or visual media . . . of the candidate with the intent to injure the candidate’s reputation or to deceive a voter into voting for or against the candidate.”); *see also* Langa, *supra* note 37, at 774.

167. VA. CODE ANN. § 18.2-386.2(A) (2019).

168. *Id.*

169. *See generally* Matthew F. Ferraro, *Deepfake Legislation: A Nationwide Survey—State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media*, WILMERHALE (Sept. 25, 2019), <https://www.jdsupra.com/post/contentViewerEmbed.aspx?fid=11861a56-5e23-4f9e-8263-ddaa20c2c1c3>.

170. *See id.*

171. *See* CAL. CIV. CODE § 1708.86 (West 2021).

172. *Id.*

intimate images.<sup>173</sup> Under this act, in addition to making the sharing of digitally altered intimate images a criminal offense, Rep. Morelle's legislation would also allow victims to sue offenders in civil court. While recent polling by the Artificial Intelligence Policy Institute shows that Americans seem to overwhelmingly support legal action against deepfakes, there has been no action taken on the bill since its introduction.<sup>174</sup>

The latest conversation surrounding the regulation of sexually-explicit deepfakes arose in January 2024 after deepfake pornographic images of Taylor Swift were posted on X.<sup>175</sup> Consequentially, a bipartisan group of three senators plans to introduced the Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024 (The DEFIANCE Act), allowing victims of non-consensual intimate AI deepfakes to take civil action against anyone who produced, possesses, or intend to distribute such material.<sup>176</sup> While no further steps have been taken in solidifying the DEFIANCE Act, it acknowledges the dangerous real-world consequences of deepfake victimization, recognizing the need to safeguard a victim's privacy through legal proceedings. Due to Swift's major popularity, the DEFIANCE Act stands as a true beacon of hope for the fight against non-consensual exploitation, signaling a unified effort by

---

173. Rep. Morelle has previously introduced the bill but has since added Rep. Tom Kean, Jr. (NJ-o7) from New Jersey as a co-sponsor after previously introducing a bill called the AI Labeling Act of 2023. Preventing Deepfakes of Intimate Images Act, H.R. 3106, 118th Cong. (2023); Press Release, Rep. Tom Kean, Jr, House of Representatives, Kean Takes Action to End AI Generated Deepfake Pornography (Jan. 16, 2024), <https://kean.house.gov/media/press-releases/kean-takes-action-end-ai-generated-deepfake-pornography> [<https://perma.cc/C3AX-NAAS>].

174. *Id.*; see also Solcyré Burga, *How a New Bill Could Protect Against Deepfakes*, TIME (Jan. 31, 2024, 4:34 PM), <https://time.com/6590711/deepfake-protection-federal-bill/> [<https://perma.cc/4KPX-874D>].

175. Kat Tenbarge, *Deepfake Bill Would Open Door for Victims to Sue Creators*, NBC NEWS (Jan. 30, 2024, 2:46 PM), <https://www.nbcnews.com/tech/tech-news/deepfake-bill-open-door-victims-sue-creators-rcna136434> [<https://perma.cc/APE8-87HX>].

176. U.S. Senate Majority Whip Dick Durbin (D-IL), U.S. Senator Lindsey Graham (R-SC), and U.S. Senators Amy Klobuchar (D-MN) and Josh Hawley (R-MO) introduced the DEFIANCE Act to allow victims to sue those involved in the creation and distribution of sexually explicit deepfake images if the person know or recklessly disregarded that the victim did not consent to the material. Press Release, Sen. Dick Durbin, Durbin, Graham, Klobuchar, Hawley Introduce DEFIANCE Act To Hold Accountable Those Responsible For The Proliferation Of Nonconsensual, Sexually-Explicit "Deepfake" Images And Videos (Jan. 30, 2024), <https://www.durbin.senate.gov/newsroom/press-releases/durbin-graham-klobuchar-hawley-introduce-defiance-act-to-hold-accountable-those-responsible-for-the-proliferation-of-nonconsensual-sexually-explicit-deepfake-images-and-videos> [<https://perma.cc/44ZD-AMVD>].

legislatures and fans of the artist to defend the dignity of individuals impacted by such digital threats.

## V. CONCLUSION

Although the path towards regulation seems brighter with the rise of targeted legislation, deepfakes still present significant, real harm to individuals across the nation. Pornographic deepfakes are particularly concerning, as they strictly exploit the privacy and agency of their primary targets: women. The use of an individual's likenesses in pornographic deepfakes not only strips them of their dignity, but it further leads to psychological and reputational damage.

To properly address the "deepfake issue," we must establish a wider, broader range of laws aimed at targeting deepfake creators to deem them civilly and criminally liable. Additionally, these potential remedies must be First Amendment and Section 230-compliant to allow victims to properly make a case under the rule of law.

As technology is constantly advancing, it is important to keep track of advancing digital manipulation tactics that enable the false publications posed by deepfakes. While deepfakes have become increasingly common in numerous social worlds such as media, politics, and entertainment, the legal system has a duty to protect victims abused by deepfake creators. Legal experts, social media participants, and internet service providers must warn the public about the dangers of deepfakes to prevent our world from turning into a false reality.