Don't Believe Your Eyes: Fighting Deepfaked Nonconsensual Pornography with Tort Law

Moncarol Y. Wang[†]

I. INTRODUCTION

Machine learning programs open the door to deepfakes: hyper-realistic, digitally falsified images and videos. Deepfakes have enhanced the art and education worlds.[1] But these beneficial uses are often dwarfed by the dominance of their harmful applications. While there is an abundance of legal scholarship on deepfakes, much of the discussion has focused on its implications in the fake news context. One scholar even argues that there appears to be a tendency to "over-focus on the theoretical possibility of deepfake-induced geopolitical instability at the expense of tackling the present threat posed by the weaponization of deepfake pornography."[2] Indeed, deepfake pornography is the real and actual test case on the ground.

This Comment will analyze deepfakes in the interpersonal context—specifically the use of technology to make deepfaked nonconsensual pornography ("DNCP"). Because deepfake images and videos appear so real, the scale of potentially negative impact is especially alarming. The accessibility of deepfaking technology means that even the private individual is at great risk of being a victim of DNCP, which can cause both internal mental-emotional distress and external employment consequences.[3] The messaging app Telegram, for instance, has

[†] B.S., 2018, University of California, Berkeley; J.D. Candidate, 2023, The University of Chicago Law School. Thanks to Professor Brian Leiter and the team at The University of Chicago Legal Forum for advice throughout the Comment process.

[1] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1769–70 (2019).

[2] *See* Judi Germano, distinguished fellow, N.Y. Univ. Ctr. for Cybersecurity, remarks at N.Y. Univ. panel: The Front Line: Big Tech, Fake News, and Private Industry's Deepfake Detection Problem (June 30, 2020), https://www.youtube.com/watch?v=iL-QmxMKcCo&list=PLJkLD_s9pYaZU_FpkX_kmH1jh0wjxgM08&index=2 [https://perma.cc/RP2D-XGR7]

[3] Chesney & Citron, *supra* note 1, at 1773–75.

been used to digitally strip 100,000 women and girls, including underage girls, of their clothing.[4] Sensity AI, a research company that has been tracking online deepfakes since late 2018, found that between 90% and 95% of all deepfake videos on the Internet are of DNCP.[5] Of that slice, 90% is DNCP of women.[6]

DNCP is a recent digital development similar to the print publication of nonconsensual pornography ("NCP").[7] With NCP, women would sue a magazine for publishing images of their naked bodies in sexually explicit poses without consent.[8] Some of these images were stolen from the victims; others were submitted by former lovers.[9] In any event, such privacy violations led the victims to suffer immense psychological harm.[10]

Whereas NCP captures a scene that happened in real life, DNCP fabricates a scene that never occurred. Instead of sharing a pre-existing image or video, a DNCP creator uses artificial intelligence to create entirely new digital content.[11] By training a machine learning program with genuine input data, the creator stitches one person's face onto another person's body.[12]

A natural place to start seeking a solution is in criminal law. While criminal law's deterrent function demonstrates some progress in reducing the likelihood of victimization through DNCP, its effectiveness is rocky at best.[13] Congress has not passed legislation squarely addressing NCP or DNCP, prompting states to act on their own. The result is a patchwork of different rules, and implementation is inconsistent given the realities of local law enforcement's priorities and the phenomenon of victim blaming.

This Comment argues that the solution to making whole the victims of DNCP lies in civil law, specifically tort law. While defamation,

---

[4] Matt Burgess, *The Biggest Deepfake Abuse Site Is Growing in Disturbing Ways*, WIRED (Dec. 15, 2021), https://www.wired.com/story/deepfake-nude-abuse [https://perma.cc/4BSD-X8HA].

[5] 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/Y5GE-PWG9].

[6] *Id.*

[7] Diane Bustamante, *Florida Joins the Fight Against Revenge Porn: Analysis of Florida's New Anti-Revenge Porn Law*, 12 FIU L. REV. 357, 359 (2017).

[8] *See* cases cited *infra* note 45.

[9] *See* Bustamante, *supra* note 7, at 360–63.

[10] Wood v. Hustler Mag., Inc., 736 F.2d 1084, 1086 (5th Cir. 1984).

[11] Rebecca A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*, 88 FORDHAM L. REV. 887, 889–91 (2019).

[12] Anna Yamaoka-Enkerlin, *Disrupting Disinformation: Deepfakes and the Law*, 22 N.Y.U. J. LEGIS. & PUB. POL'Y 725, 726 (2020).

[13] *See* discussion *infra* part D.

publicity in false light, and intrusion on seclusion are applicable to certain narrow fact patterns, intentional infliction of emotional distress with its proven track record in the NCP context makes it the most powerful theory for DNCP victims.

Part II of this Comment traces the development of deepfakes, illustrates their applications, and explains how attempts to police them via criminal statutes have fallen short. Part III evaluates current remedies, including detection technology, with a focus on those provided by torts. Of the torts I explore, the intentional infliction of emotional distress tort may be the best litigation strategy to address DNCP, with some caveats. It raises some First Amendment defenses, although the rationale justifying protection does not hold water in the DNCP context. And, under some specific fact patterns, other dignitary torts may be more effective. Despite this, the catch-all quality of the intentional infliction of emotional distress would provide DNCP victims with tools to be made whole despite the lack of specific statutory protections.

II. THE DEEPFAKE LANDSCAPE

A. Deepfake Technology

In 2015, Google released to the public TensorFlow, a platform offering tools to build machine learning models.[14] The underlying technology is believed to have been created by Ian Goodfellow, currently a Director of Machine Learning in the Special Projects Group at another tech giant, Apple.[15] These machine learning models are the building blocks for artificial intelligence ("AI") algorithms.[16] AI technology allows users to create seemingly authentic digital content, for example deepfakes. A portmanteau of "deep learning" and "fake,"[17] deepfakes first went viral in 2017 when an account user by the name of @deepfakes posted a digitally falsified video created with TensorFlow to Reddit, a

[14] TENSORFLOW, https://www.tensorflow.org/ [https://perma.cc/HQ2R-WJ3U] (last visited July 29, 2022).

[15] *See* Martin Giles, *The GANfather: The Man Who's Given Machines the Gift of Imagination*, MIT TECH. REV. (Feb. 21, 2018), https://www.technologyreview.com/2018/02/21/145289/the-ganfather-the-man-whos-given-machines-the-gift-of-imagination/ [https://perma.cc/7GG5-NG5Q].

[16] *See* Dave Gershgorn, *Google Gave the World Powerful AI Tools, and the World Made Porn with Them*, QUARTZ (Feb. 7, 2018), https://qz.com/1199850/google-gave-the-world-powerful-open-source-ai-tools-and-the-world-made-porn-with-them [https://perma.cc/Q432-BDQ4].

[17] Manh Hung Tran, *Deep Fakes and the Handling of the Next Frontier of Fake News and Human Agency Erosion*, CONNECT ON TECH (Feb. 21, 2022), https://www.connectontech.com/deep-fakes-and-the-handling-of-the-next-frontier-of-fake-news-and-human-agency-erosion [https://perma.cc/Y76F-ESLC].

social media website.[18] This video depicted actress Gal Gadot's face, superimposed onto an actual pornography actress's body.[19]

1. How to Create a Deepfake

To produce a deepfake, a creator inputs genuine photo, video, and audio files of different people into a machine learning program.[20] The artificial intelligence within the program reviews these inputs, called the "faceset," and trains itself to recognize patterns in each individual's tone, cadence, inflection, and movements.[21] The creator then instructs the program to map one person's physical and auditory characteristics onto another person's body.[22] The end product is a scene of someone saying or doing something that never actually occurred in real life.

2. Application of Deepfake Technology

There are many examples of how deepfake technology can be used to promote expression. For example, Hollywood uses deepfakes to make films starring actors who have passed away.[23] It brought to life a speech that John F. Kennedy never delivered due to his assassination.[24] The technology also has the potential to make dubbing of foreign language films more realistic.[25] Children's educational television shows include deepfaked historical characters to enrich the lessons.[26] Museum curators feature life-size deepfakes of important figures on digital screens to supplement their exhibits.[27] Mental health patients can use a live,

---

[18] *See* Samantha Cole, *AI-Assisted Fake Porn Is Here and We're All Fucked*, MOTHERBOARD (Dec. 11, 2017), https://motherboard.vice.com/en_us/article/gydydm/gal-gadot-fake-ai-porn [https://perma.cc/4SUT-W3Z6].

[19] Lindsey Wilkerson, *Still Waters Run Deep(fakes): The Rising Concerns of "Deepfake" Technology and Its Influence on Democracy and the First Amendment*, 86 MO. L. REV. 407, 409 (2021).

[20] *See generally* Russell Spivak, *"Deepfakes": The Newest Way to Commit One of the Oldest Crimes*, 3 GEO. L. TECH. REV. 339, 341 (2019).

[21] Beatrice Hazlehurst, *AI-Generated Celebrity Porn May Be Including Child Actors*, PAPER MAGAZINE (Feb. 28, 2018), https://www.papermag.com/deep-fake-child-porn-2540933488.html [https://perma.cc/92FU-4S5Z].

[22] *See* Yamaoka-Enkerlin, *supra* note 12, at 731.

[23] Reasonable minds disagree on whether this is a desirable way of maintaining the star's legacy, especially when the family does not consent. *See, e.g.*, Julia Jacobs, *Bourdain Documentary's Use of A.I. to Mimic Voice Draws Questions*, N.Y. TIMES (July 16, 2021), https://www.nytimes.com/2021/07/16/movies/anthony-bourdain-ai-voice.html [https://perma.cc/YNP2-NYSC].

[24] *JFK Unsilenced*, CEREPROC, https://www.cereproc.com/en/jfkunsilenced [https://perma.cc/K7BB-3B4U] (last visited July 29, 2022).

[25] Nina I. Brown, *Deepfakes and the Weaponization of Disinformation*, 23 VA. J.L. & TECH. 1, 33 (2020).

[26] Chesney & Citron, *supra* note 1, at 1769.

[27] Dami Lee, *Deepfake Salvador Dalí Takes Selfies with Museum Visitors*, VERGE (May 10, 2019), https://www.theverge.com/2019/5/10/18540953/salvador-dalilives-deepfake-museum [https://perma.cc/9M8P-T975].

real-time deepfake avatar to receive telehealth treatment, which avoids any potential stigma or biases from the healthcare provider.[28] There is even evidence that ALS patients and other individuals suffering from similar forms of paralysis can use deepfakes to speak with their own voice via vocal avatars.[29] All these examples form an impressive list of how deepfake technology promotes expression in a variety of contexts and its pro-social benefits.

But other deepfakes, created without the consent of the depicted individuals, are not so beneficial. To some, they are "one of the cruelest, most invasive forms of identity theft invented in the internet era."[30] In an increasingly connected world, where seeing is believing, deepfakes are especially ruthless tools of extortion and sabotage.[31] For instance, some scammers in India use fraudulent social media profiles to lure victims into video calls.[32] Then, the scammers use deepfaked pornography to encourage explicit behavior by the victims, record that behavior, and then use it to blackmail the victim (even creating deepfakes of the victims themselves).[33]

These examples demonstrate how the epistemological priority of sight—trusting what we see with our own eyes to be the uncontested truth[34]—leads to problematic results. It is hard to beat the power of story captured on film to serve as conclusive proof. Deepfake videos are especially sharp weapons, given the multi-sensory experience they generate. Because deepfakes "exploit the natural human tendency to rely on observation through [bodily] senses such as sight and sound," the public potentially gives even suspicious deepfakes the benefit of the doubt and may believe them to be real.[35]

Not only is deepfake technology powerful, given its wide spectrum of application, but it has also become more and more accessible. The Internet is enormous, anonymous, and instant. This accessibility means that private individuals are both increasingly able to wield enormous power over victims and increasingly at risk of becoming deepfakes' next

---

[28] Damon Beres & Marcus Gilmer, *A Guide to 'Deepfakes,' the Internet's Latest Moral Crisis*, MASHABLE (Feb. 2, 2018), https://mashable.com/2018/02/02/what-are-deepfakes/#dnpjFgfXHqqb [https://perma.cc/QW9V-5532].

[29] Chesney & Citron, *supra* note 1 at 1771.

[30] Franklin Foer, *The Era of Fake Video Begins*, ATLANTIC (May 2018), https://www.theatlantic.com/magazine/archive/2018/05/realitys-end/556877 [https://perma.cc/DGE8-Q9QS].

[31] Chesney & Citron, *supra* note 1, at 1774.

[32] Yana Pashaeva, *Scammers Are Using Deepfake Videos Now,* SLATE (Sept. 13, 2021), https://slate.com/technology/2021/09/deepfake-video-scams.html [https://perma.cc/QT28-27JU].

[33] *Id.*

[34] *See* Jenni Lauwrens, *Can You See What I Mean? An Exploration of the Limits of Vision in Anti-Ocularcentric Contemporary Art*, 85 DE ARTE 26, 28 (2012).

[35] Elizabeth Caldera, *"Reject the Evidence of Your Eyes and Ears": Deepfakes and the Law of Virtual Replicants*, 50 SETON HALL L. REV. 177, 187 (2019).

subjects themselves. Unlike Adobe Photoshop, which requires expensive software and a certain level of technical skill necessary for manual editing, deepfake programs are cheap and beginner-friendly.[36] Even I, equipped with "a single source photo and zero technical experience," could create a deepfake avatar with an application on my iPhone.[37] Thousands of Reddit users and a New York Times journalist have done precisely that.[38] And a creator need not manually gather the faceset.[39] Open-source tools like DownAlbum and Instagram Scraper download all images of an individual from his or her social media accounts to create the faceset.[40] Those with more technical experience can tinker with building their own deepfake program using open-source software available online.[41] Developers have created mobile phone apps, meaning an average non-expert can manipulate videos with a few taps.[42] There even exists a cottage industry where customers can hire deepfake creators to produce deepfakes for as little as twenty dollars.[43]

---

[36] *See* Spivak, *supra* note 20, at 349–50.

[37] Geoffrey A. Fowler, *Anyone with an iPhone Can Now Make Deepfakes. We Aren't Ready For What Happens Next.*, WASH. POST (Mar. 25, 2021), https://www.washingtonpost.com/technology/2021/03/25/deepfake-video-apps [https://perma.cc/6NMG-JDAL]. *See also* Brooklynn Armesto-Larson, *Nonconsensual Pornography: Criminal Law Solutions to A Worldwide Problem*, 21 OR. REV. INT'L L. 177, 195–96 (2020).

[38] Adam Dodge et al., *Using Deep Fake Technology to Perpetrate Intimate Partner Abuse*, CAL. P'SHIP TO END DOMESTIC VIOLENCE 6 (2018), https://www.cpedv.org/sites/main/files/webform/deepfake_domestic_violence_advisory.pdf [https://perma.cc/J8QL-95AP]; Kevin Roose, *Here Come the Fake Videos, Too*, N.Y. TIMES (Mar. 4, 2018), https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html [https://perma.cc/3927-AW3H].

[39] A faceset is a set of images used to create a deepfake. Samantha Cole, *Fake Porn Makers Are Worried About Accidentally Making Child Porn,* VICE (Feb. 27, 2018), https://www.vice.com/en/article/evmkxa/ai-fake-porn-deepfakes-child-pornography-emma-watson-elle-fanning [https://perma.cc/HL8D-AFQ5].

[40] Douglas Harris, *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, 17 DUKE L. & TECH. REV. 99, 101 (2019).

[41] *See* Spivak, *supra* note 2020, at 349.

[42] *See, e.g.*, Ivan Mehta, *New Deepfake App Pastes Your Face onto GIFs in Seconds*, NEXT WEB (Jan. 13, 2020), https://thenextweb.com/news/new-deepfake-app-pastes-your-face-onto-gifs-in-seconds [https://perma.cc/E4CV-DEB5]; Zak Doffman, *Chinese Deepfake App ZAO Goes Viral, Privacy of Millions 'At Risk'*, FORBES (Sept. 2, 2019), https://www.forbes.com/sites/zakdoffman/2019/09/02/chinese-best-ever-deepfake-app-zao-sparks-huge-faceapp-like-privacy-storm/?sh=27b354bf8470 [https://perma.cc/92D9-ENVZ].

[43] Drew Harwell, *Fake-Porn Videos Are Being Weaponized to Harass and Humiliate Women: "Everybody Is a Potential Target",* WASH. POST (Dec. 30, 2018), https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target [https://perma.cc/5L7L-XS6U].

B. Deepfaked Nonconsensual Pornography

1. History

One particularly problematic application of deepfake technology is DNCP. DNCP can be traced to the broader general phenomenon of nonconsensual pornography ("NCP"). NCP is the act of sharing a private, sexually explicit, genuine image or video without the consent of the depicted individual.[44] NCP emerged in the 1980s when Hustler Magazine began publishing nude, reader-submitted photographs of "nonprofessional female models" in its "Beaver Hunt" column.[45] Although the magazine required consent forms, forgeries went undetected because there was no formal procedure to ensure their accuracy or authenticity.[46] With modern-day NCP, sometimes the content is stolen via hacking into the victim's device.[47] Other times it is shared nonconsensually by a prior romantic partner, as was often the case with Hustler Magazine.[48]

NCP is commonly called "revenge pornography," though leading cyber-harassment scholars argue that the moniker is misleading and undermines its harmful effects.[49] "Revenge pornography" over-emphasizes the explicit nature of the content, suggesting that sexuality is shameful, and only captures a specific scenario of abuse.[50] Not all revenge pornography is revenge-driven. Other motives include entertainment, profit, or notoriety.[51] One 2017 study by the Cyber Civil Rights Initiative found that 79% of those who shared NCP said they did not mean to hurt the individuals depicted.[52] For these reasons, scholars Clara McGlynn and Erika Rackle suggest that using the term "image-based sexual abuse" would better focus the law on the wrongful act it-

---

[44] Caroline Drinnon, *When Fame Takes Away the Right to Privacy in One's Body: Revenge Porn and Tort Remedies for Public Figures*, 25 WM. & MARY J. WOMEN & L. 209, 211 (2017).

[45] *See*, *e.g.*, Wood v. Hustler Mag., Inc., 736 F.2d 1084, 1086 (5th Cir. 1984); Ashby v. Hustler Mag., Inc., 802 F.2d 856, 857–58 (6th Cir. 1986).

[46] *Wood*, 736 F.2d at 1086.

[47] Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1917–18 (2019).

[48] *Id.*

[49] *See generally* Clare McGlynn & Erika Rackley, written submission to Scotland's Justice Committee on Abusive Behaviour and Sexual Harm Bill (Nov. 5, 2015), https://archive2021.parliament.scot/S4_JusticeCommittee/Inquiries/ABSH3._McGlynn_and_Rackley.pdf [https://perma.cc/EYM5-KEWG].

[50] *Id.*

[51] Mary Anne Franks, *Why Revenge Porn Must be a Crime: Dissecting Critics' Attempts to Nitpick Important Legislation*, N.Y. DAILY NEWS (Feb. 26, 2014), http://www.nydailynews.com/opinion/revenge-porn-crime-article-1.1702725 [https://perma.cc/Z6R5-AJVZ].

[52] Michelle Gonzalez, *Nonconsensual Porn: A Common Offense*, CYBER C.R. INITIATIVE (June 12, 2017), https://www.cybercivilrights.org/2017-natl-ncp-research-results [https://perma.cc/GHX9-D4LX].

self, which is the disseminator's breach of trust, and avoid fueling victim blaming.[53] What is important is not the consensually created image but the fact that the distributor exceeded the bounds of that initial consent when subsequently sharing it.

NCP is widely shared digitally, typically via social media platforms, emails, and text messages.[54] In 2009, someone changed the Facebook profile picture of Holly Jacobs, then a college student, into a nude photograph of herself.[55] She confronted her ex-boyfriend, the only person with whom she shared such photos, who denied involvement and claimed he was hacked.[56] Nowadays, NCP is available both on NCP-exclusive websites and on more mainstream pornography websites.[57] The Cyber Civil Rights Initiative found that 15.8% of all women reported having been victimized by or threatened with NCP.[58]

DNCP, a more recent development, is NCP in the artificial intelligence age. Like NCP, DNCP involves a sexually explicit image shared without consent. But whereas NCP images are authentic, DNCP images are doctored to depict scenes that never happened in real life. As with deepfakes more generally, DNCP is created using an artificial intelligence program's iterative learning process. DNCP takes NCP's lack of consent one step further. The actor not only lacks the depicted individual's consent for the *distribution* of the doctored image but also lacks consent for the creation of the doctored image in the first place.[59]

2. Dangers to Victims

Victims of DNCP commonly experience mental distress and emotional embarrassment.[60] Although celebrity DNCP is a frequent use of deepfake technology to date,[61] the ease and accessibility of deepfakes—and thus of DNCP—ratchets up the likelihood of everyday people serving as a target of a DNCP campaign. Plus, NCP actors have also developed ways to take advantage of search engine algorithms so that search

---

[53] McGlynn & Rackley, *supra* note 49.

[54] Mary Anne Franks, *Revenge Porn Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251, 1260–61 (2017).

[55] Michael E. Miller, *Miami Student Holly Jacobs Fights Revenge Porn*, MIA. NEW TIMES (May 9, 2013), http://www.miaminewtimes.com/news/miami-student-holly-jacobs-fights-revenge-porn-6392040 [https://perma.cc/B8U4-TAZF].

[56] *Id.*

[57] *See* Armesto-Larson, *supra* note 37, at 183.

[58] Gonzalez, *supra* note 52.

[59] Delfino, *supra* note 11, at 890.

[60] Delfino, *supra* note 11, at 897.

[61] Kristen Dold, *Face-Swapping Porn: How a Creepy Internet Trend Could Threaten Democracy*, ROLLING STONE (Apr. 17, 2018), https://www.rollingstone.com/culture/culture-features/face-swapping-porn-how-a-creepy-internet-trend-could-threaten-democracy-629275 [https://perma.cc/6P7Z-RUVR]; Beres & Gilmer, *supra* note 28.

results for a particular person will result in NCP populating first.[62] There is no reason to think this practice has not already been implemented for DNCP. An innocent Google search to find someone's social media presence may lead to the discovery of a DNCP campaign, complicating the interpersonal relationship.

Given that the targets are overwhelmingly female,[63] DNCP exploits and further stigmatizes female sexuality. Such misogynistic abuse discourages female participation in the digital space, which reduces the quality of public discourse.[64] For example, following a television interview where investigative journalist Rana Ayyub criticized the Indian prime minister, someone targeted Ayyub with a DNCP video in which her face was overlaid onto the body of a different woman engaged in sex.[65] As the DNCP went viral, online harassment spilled over into real-life complications—the turmoil resulted in her hospitalization for heart palpitations.[66]

In addition to psychological impact, DNCP generates serious external consequences, particularly in the employment market. A Microsoft study found that almost 80% of employers use search results to make hiring decisions.[67] First impressions are influential. If employers come across nude photographs, they are unlikely to follow up with the candidates and inquire whether those photographs were the results of NCP or DNCP.[68] Even if the prospective employer understands that the photos are fake, seeing "the pornographic depictions may taint their view of these women, just as knowledge of a rape victim's identity often colors

---

[62] DANIELLE CITRON, HATE CRIMES IN CYBERSPACE 70 (2014).

[63] Deeptrace Labs created a service to identify deepfakes and found that 96% of the subjects of these fake videos are women. Aja Romano, *Deepfakes Are a Real Political Threat. For Now, Though, They're Mainly Used to Degrade Women*, VOX (Oct. 7, 2019), https://www.vox.com/2019/10/7/20902215/deepfakes-usage-youtube-2019-deeptrace-research-report [https://perma.cc/XA9F-SFY6].

[64] *See* Harwell, *supra* note 43; Marjan Nadim & Audun Fladmoe, *Silencing Women? Gender and Online Harassment*, 39 SOC. SCI. COMPUT. REV. 245, 245–46 (2019).

[65] Ben Christopher, *Can California Crack Down on Deepfakes Without Violating the First Amendment?*, CAL MATTERS (July 2, 2019), https://calmatters.org/politics/2019/07/deepfake-berman-california-politics-ab730-fake-news-first-amendment/ [https://perma.cc/8NWE-KL7B]. *See also* Rana Ayyub, *I Was the Victim of a Deepfake Porn Plot Intended to Silence Me*, HUFFPOST (Nov. 21, 2018), https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316 [https://perma.cc/352B-8CR4].

[66] Ayyub, *supra* note 65.

[67] Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 352 (2014).

[68] *Id.*

people's associations with her."[69] Instead, employers are likely to pursue the path of least resistance, moving on to other candidates who are less likely to reflect poorly on the employer.[70]

C. Landscape of Statutory Remedies

Because deepfakes pose great risks to the public, criminal liability makes sense to achieve deterrence. But there is no federal law criminalizing NCP or DNCP.[71] As a result, actors are either prosecuted under indirectly related federal laws or under state law.[72] Even where criminal law does cover NCP and DNCP, it is inadequate due to enforcement issues. This is explained in detail below.

1. Tangential Federal Laws

Congress has passed legislation regulating activity on the Internet that may extend to DNCP. Federal cyberstalking laws like the Interstate Anti-Stalking Punishment and Prevention Act make it a felony to use any "interactive computer service or electronic communication service . . . to engage in a course of conduct that . . . causes, attempts to cause, or would reasonably be expected to cause substantial emotional distress to a person . . . ."[73] This law might be stretched to reach DNCP, but it is likely of limited use for one-off NCP and DNCP cases for two reasons. First, the law requires that the actor "have an intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person."[74] Actors who prove some other objective besides intent to harm—such as humor—would not satisfy the intent requirement. Second, sanctions have so far been reserved for actors who are consistent in their harassment.[75]

The Computer Fraud and Abuse Act prohibits computer hacking and the distribution of information obtained from it.[76] This statute is helpful in the rare cases where NCP or DNCP is obtained or created from computer hacking.

---

[69] Martha C. Nussbaum, *Objectification and Internet Misogyny*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 80 (Saul Levmore & Martha C. Nussbaum eds., 2010).

[70] *Id.*

[71] Karla Utset, *Drawing the Line: The Jurisprudence of Non-Consensual Pornography and the Implications of Kanye West's Famous Music Video*, 72 U. MIA. L. REV. 920, 925 (2018).

[72] *See generally id.*

[73] 18 U.S.C. § 2261A(2).

[74] *Id.*

[75] Salina Tariq, *Revenge: Free of "Charge?"*, 17 SMU SCI. & TECH. L. REV. 227, 244 (2014).

[76] 18 U.S.C. § 1030.

The Video Voyeurism Prevention Act of 2004 punishes "the intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy."[77] This Act potentially applies to DNCP, as the statutory definition of "capture" includes "to electronically transmit a visual image with the intent that it is viewed," but it may be underinclusive with respect to actors who merely produce DNCP.[78]

The Copyright Act of 1976 grants the original creator of works of authorship five exclusive rights: to reproduce, to create derivative works, to distribute, to perform, and to display.[79] Because copyright protection is only available where the work is created by the victim, this solution is of limited efficacy.[80] In the NCP context, it is more likely that the victim is also the creator of the work of authorship—she[81] took a nude photo of herself—and this is the case for about 80% of all NCP victims.[82] However with DNCP, the victim may have personally taken the original photos in the faceset—so she may be able to assert copyright over these source images—but she did not "take" the deepfaked photo. Moreover, the artificial nature of the doctored content makes for a more forceful case of the fair use exception. Under this exception, the actor has a strong affirmative defense to a copyright violation in situations where he did not financially benefit from the DNCP.[83] In any event, copyright law is meant to incentivize creation by granting a monopoly to protect an author's commercial interests in his or her work, not to protect from emotional harm.[84]

2. Attempts at Targeted Federal Laws

The only successfully enacted federal legislation related to deepfakes is the National Defense Authorization Act for Fiscal Year 2020.[85] But this act does not establish criminal liability. Rather, it requires that the Director of National Intelligence submit a report to congressional

---

[77] 18 U.S.C. § 1801(a).

[78] 18 U.S.C. § 1801(b)(1)–(2).

[79] 17 U.S.C. §§ 106, 107–22.

[80] Citron, *supra* note 62, at 122.

[81] Throughout this Comment, I will refer to the defendant as "he" and the plaintiff as "she" given that DNCP is largely a gendered problem.

[82] Tariq, *supra* note 75, at 244; Jenna K. Stokes, *The Indecent Internet: Resisting Unwarranted Internet Exceptionalism in Combating Revenge Porn*, 29 BERKELEY TECH. L.J. 929, 941 n.80 (2014).

[83] *See* Chesney & Citron, *supra* note 1, at 1793.

[84] *See* Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985) ("By establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas.").

[85] 50 U.S.C. § 3369a.

intelligence committees detailing the potential national security impacts of machine-manipulated media and allows the director to award grants for research of deepfake detection technology.[86]

Additionally, several attempts to criminalize deepfakes have stalled over worries that they were too broad, risking violations of the First Amendment.[87] For instance, Senator Benjamin Sasse of Nebraska introduced the Malicious Deepfake Prohibition Act of 2018, which would have made it illegal to "create, with the intent to distribute, a Deepfake with the intent that the distribution of the Deepfake would facilitate criminal or tortious conduct."[88] But it has not moved past committee.[89]

New York Representative Yvette Clark introduced the DEEP FAKES Accountability Act,[90] which would have instituted several initiatives to regulate such content and protect victims. First, it would have required anyone creating a deepfake to watermark the deepfake with a label stating it had been altered.[91] Second, it would have created criminal and civil liability for failing to disclose the videos' altered nature.[92] Third, the bill outlined a framework for enforcement and victim assistance, requiring the Attorney General to place a coordinator in each U.S. Attorney's Office to receive reports of deepfakes from foreign nations and coordinate prosecutions.[93] Finally, a Deep Fakes Task Force would have been created within the Department of Homeland Security to address deepfakes' national security impact.[94] However, the bill has not progressed since being referred to a subcommittee.[95]

Senator Robert Portman of Ohio introduced the Deepfake Report Act of 2019,[96] which was passed in the Senate but stalled in the House.[97] The bill would have required the Department of Homeland Security to

---

[86] 50 U.S.C. § 3024.

[87] *See* Jessica Ice, *Defamatory Political Deepfakes and the First Amendment*, 70 CASE W. RES. L. REV. 417, 431 (2019).

[88] S. 3805, 115th Cong. (2018).

[89] *Actions Overview S.3805–115th Congress (2017-2018)*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/senate-bill/3805/actions?KWICView=false [https://perma.cc/WGY4-Y94Q] (last visited July 31, 2022).

[90] H.R. 3230, 116th Cong. (2019).

[91] *Id.* at § 2(a).

[92] *Id.*

[93] *Id.*

[94] *Id.* at § 6(a).

[95] *All Actions H.R.3230–116th Congress (2019-2020)*, CONGRESS.GOV, https://www.congress.gov/bill/116th-congress/house-bill/3230/all-actions [https://perma.cc/J74G-5Z3Y] (last visited July 31, 2022).

[96] S. 2065, 116th Cong. (2019).

[97] *Actions Overview S.2065–116th Congress (2019-2020)*, CONGRESS.GOV, https://www.congress.gov/bill/116th-congress/senate-bill/2065/actions?KWICView=false [https://perma.cc/42GK-5YVG] (last visited July 31, 2022).

report periodically on the "state of digital content forgery technology" and conduct relevant public hearings to gather information as part of that process.[98]

3. Targeted State Laws

On the state side, forty-eight states and the District of Columbia have statutes criminalizing NCP.[99] States with NCP laws vary in assigning the severity of the offense—misdemeanor or felony—and characterizing the harm—e.g., as a type of violation of privacy or of harassment, or simply as a stand-alone category of offense.[100]

Currently, three states have laws explicitly targeting deepfakes. In Virginia, anyone who shares DNCP of someone else is subject to a misdemeanor[101] that may come with twelve months in jail and a $2,500 fine.[102] Meanwhile, California has enacted a private cause of action against the DNCP distributor.[103] Texas law criminalizes the creation and distribution of deepfake videos, but only those intended to harm candidates running for office during elections.[104]

D. The Shortcomings of Current Criminal Statutes

The wide coverage of NCP under state law, while promising, does not mean that these cases are readily addressed. Given the inefficacy of such NCP laws for NCP *itself*,[105] seeking relief for DNCP victims via NCP laws—on the theory that both involve nonconsensual acts and reputational damage—is likely insufficient. Even where there are targeted DNCP laws, resource constraints and the tendency to victim blame challenge enforcement.

1. Resource and Jurisdiction Constraints

Although law enforcement agencies have large investigative capacities, these capacities may not be deployed due to resource constraints,

---

[98] S. 2065, 116th Cong. § (3)(a), (c).

[99] *48 States + DC + One Territory Now Have Revenge Porn Laws*, CYBER C.R. INITIATIVE, https://cybercivilrights.org/nonconsensual-pornography-laws/ [https://perma.cc/DFT4-RW8C] (last visited July 31, 2022).

[100] *See* Armesto-Larson, *supra* note 37, at 199–201.

[101] VA. CODE ANN. § 18.2-386.2.A.

[102] VA. CODE ANN. § 18.2-11.

[103] CAL. CIV. CODE § 1708.85(b).

[104] TEX. ELECTION CODE ANN. § 255.004 (West 2019) ("A person commits an offense if the person, with intent to injure a candidate or influence the result of an election: (1) creates a deep fake video; and (2) causes the deep fake video to be published or distributed within 30 days of an election.").

[105] *See* discussion *infra* part D.

internal priorities, and external politics resulting in underenforcement.[106] Local police departments sometimes dismiss victims by saying the online activity was legal or that they lack jurisdiction.[107] In Holly Jacobs's case, the local police department said there was nothing they could do as she was over eighteen, and her ex-boyfriend did not technically steal the photographs from her.[108] Some Federal Bureau of Investigation agents say this type of interpersonal online abuse is not related to national security, and thus they cannot help.[109] The Department of Justice's Computer Crimes and Intellectual Property Section has the investigative techniques necessary to identify online perpetrators, but "their capabilities do not scale easily."[110] There is also the risk that district attorneys will prosecute to promote their self-interests rather than the interests of the victims.[111]

2. Victim Blaming

Furthermore, some socially held attitudes prevent people from taking victims' requests for help seriously. Victim blaming abounds, especially in the NCP context, where often the initial creation of the media may have been consensual.[112] The invasion of privacy was of the victim's own making, and the solution is apparently simple: "[p]eople just have to grow up in terms of what they're taking and loading on to the computer because the risk is so high."[113] The underlying logic is that "if you do not take pictures or videos of yourself or allow others to take them, then you will not have a problem."[114] Even in the DNCP context, where it is clear that the victim did not consent to the inherently false image, victim blaming is an obstacle.[115]

But advising victims to self-help or to go offline because "boys will be boys,"[116] ignores the reality that images are taken constantly in today's connected world.[117] It also dismisses the "gendered nature of the

---

[106] *See* Chesney & Citron, *supra* note 1, at 1801.

[107] *See* Citron, *supra* note 62, at 47.

[108] Miller, *supra* note 55.

[109] Citron, *supra* note 62, at 47.

[110] Chesney & Citron, *supra* note 1, at 1801.

[111] *Id.* at 1789.

[112] Citron, *supra* note 62, at 78.

[113] Shalailah Medhora, *Senate Committee Recommends the Criminalisation of Revenge Porn*, GUARDIAN (Feb. 25, 2016), https://www.theguardian.com/australia-news/2016/feb/25/senate-committee-recommends-the-criminalisation-of-revenge-porn [https://perma.cc/WPT7-9VP2].

[114] Peter W. Cooper, *The Right to Be Virtually Clothed*, 91 WASH. L. REV. 817, 819 (2016).

[115] Hao, *supra* note 5 ("The fact that faked and deepfake porn are inherently false also doesn't quiet the volume of victim blaming.").

[116] Citron, *supra* note 62, at 20.

[117] Cooper, *supra* note 114, at 819.

problem." Data suggests that NCP and DNCP disproportionately affect women.[118] Recall that the majority of deepfake videos online are DNCP and that the majority of those are of women.[119] Danielle Citron notes that perpetrators "know that women will be seen as sluts . . . . It will make them unemployable, undateable, and at risk for sexual assault."[120] It is usually men who engage in the initial act of creation or distribution, then women who suffer the consequences at the other end.[121]

III. REMEDIES

A. Detection Technology

Although this Comment focuses on ex post tort remedies, ex ante solutions are also on the table. The primary ex ante tool against DNCP is detection, which sorts between genuine and doctored media and then blocks the latter from being distributed in the first place. Nothing is ever guaranteed to be deleted from the Internet,[122] so circulation may extend perhaps indefinitely into the future. Combining this longevity with the ease of DNCP dissemination means that eradication is almost impossible without major development in detection technology.

But some crude detection methods already exist.[123] For example, some software can count the number of times someone in a video blinks, then compare that number to an average human's blink rate of fifteen to twenty times a minute.[124] The software would flag the potentially fake content—those where it counted too many or too few blinks.

---

[118] *See* Gonzalez, *supra* note 52.

[119] Hao, *supra* note 5.

[120] Citron, *supra* note 62, at 17.

[121] *Id.*

[122] Emily Perkins, *Nothing Gets Deleted on the Internet*, STARTUPS MAGAZINE, https://startupsmagazine.co.uk/article-nothing-gets-deleted-internet [https://perma.cc/HSA7-B8E6] (last visited Oct. 11, 2022). *See also* Fady Zaki, *"Innocence of Islam" Incident Proves Governments Can't Control Speech*, AM.'S FUTURE FOUND (Feb. 22, 2013), https://americasfuture.org/innocence-of-islam-incident-proves-governments-cant-control-speech/ [https://perma.cc/2EWE-FGLX].

[123] Brown, *supra* note 25, at 57.

[124] Yuezun Li et al., *In Ictu Oculi: Exposing AI Created Fake Videos by Detecting Eye Blinking*, 2018 IEEE INT'L WORKSHOP ON INFO. FORENSICS AND SEC. (Dec. 2018), https://ieeexplore.ieee.org/abstract/document/8630787 [https://perma.cc/84JP-4SHV]; Joseph Stromberg, *Why Do We Blink So Frequently?*, SMITHSONIAN MAG. (Dec. 24, 2012), https://www.smithsonianmag.com/science-nature/why-do-we-blink-so-frequently-172334883/ [https://perma.cc/AKD6-A68F].

B. Internet Companies' Incentives

Once we clear the detection technology development hurdle, the natural extension would be to convince Internet companies to implement content moderation. But it still might be difficult to persuade these companies, even those committed to stopping deepfakes, to employ detection technology at the point of upload voluntarily.[125] For example, there are considerable transaction costs in the decision between banning all deepfakes or just those with the potential to cause harm.[126] And how should these gatekeeping companies balance competing interests—such as free expression, truth, and public safety—while distinguishing between beneficial and harmful deepfakes?[127] Targeting just the latter will necessitate some level of human interpretation in making these line-drawing judgments, but humans are error-prone.

Thankfully, companies likely have independent incentives to self-police in this way. Profitability is tied to user numbers. And although Twitter and Facebook continue to be popular despite problematic posts, content moderation is key to their ability to continue attracting and retaining users in the long-run and remaining relevant figures in global communications.[128] Websites known to have robust policies in this space are commonplace in everyday life—Reddit, for example, which has since banned deepfakes and taken down the r/deepfakes subreddit page[129]—whereas completely unmoderated websites are relegated to the fringes of the Internet—8chan, 4chan, and Voat allow DNCP.[130] But until technology innovates an ex ante solution, the law must grapple with how to make these victims whole ex post.

---

[125] Brown, *supra* note 25, at 28.

[126] *Id.*

[127] Brown, *supra* note 25, at 30.

[128] Lee Rainie, Janna Anderson, and 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-offree-speech-trolls-anonymity-and-fake-news-online/ [https://perma.cc/9U2K-SXJS].

[129] Samantha Cole, *Reddit Just Shut Down the Deepfakes Subreddit*, VICE (Feb. 7, 2018), https://www.vice.com/en/article/neqb98/reddit-shuts-down-deepfakes [https://perma.cc/H3K2-2GKL].

[130] Jay Hathaway, *Here's Where 'Deepfakes,' the Fake Celebrity Porn, Went After the Reddit Ban,* DAILY DOT (May 22, 2021), https://www.dailydot.com/unclick/deepfake-sites-reddit-ban/ [https://perma.cc/367W-3FNK]. *See also* Kevin Roose, *"Shut the Site Down," Says the Creator of 8chan, a Megaphone for Gunmen*, N.Y. TIMES (Aug. 4, 2019), https://www.nytimes.com/2019/08/04/technology/8chan-shooting-manifesto.html [https://perma.cc/DQB6-2Y4H].

C. Pursuing Litigation

Litigation is the law's ex post remedy and likely the sharpest tool until detection technology catches up. But lawsuits are not silver bullets. Hiring an attorney and seeking a legal remedy is both expensive and time-consuming. Bringing a claim means reliving the nightmarish experience. Most of the time, plaintiffs may not bring their cases anonymously, meaning they expose themselves to more public scrutiny.[131] Even if the court finds for the plaintiff and orders monetary damages and a positive injunction for websites to take down the content, those remedies do little to undo the plaintiff's reputational and emotional damage.

Solutions proposed for NCP may be promising for DNCP. While it is true that the common law's incremental pace of development lags behind that of technology, common law nevertheless accommodates the fast pace of technological innovation more flexibly than statutory criminal law. Unlike a victim for NCP, a victim for DNCP arguably does not exist in real life; however, the two concepts nevertheless share sufficient commonalities to utilize the same common-law-based torts.

1. The Plaintiff Problem

Every lawsuit starts with a plaintiff. But who should bring the lawsuit? In each instance of DNCP, there are two potential plaintiffs since the depicted "person" is a fiction: (1) the source body and (2) the source face. Although the person whose body was used for the DNCP was also violated, it seems more reasonable for the person whose face was used to serve as the plaintiff. Faces are more readily identifiable than other parts of the body, so it is likely that the source face individual suffers the bulk, if not all, of the harm and thus can bring a more persuasive case.

2. The Defendant Problem and Section 230

And against whom should the lawsuit be brought? A natural starting point is to sue platforms since they have the deep pockets to pay damages, but Section 230 of the Communications Decency Act grants blanket immunity to platforms for user-generated content.[132]

Congress enacted Section 230 in response to *Stratton Oakmont, Incorporated v. Prodigy Services Company*.[133] There, the New York Supreme Court of Nassau County held that an Internet service provider's

---

[131] FED. R. CIV. P. 17(a)(1).

[132] 47 U.S.C. § 230(c).

[133] 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

exercise of editorial control over content posted on its online bulletin board made it equivalent to an offline publisher, meaning it was liable for defamatory content posted on that board.[134] Following this holding, other Internet service providers worried about potential liability for their users' posts, discouraging them from regulating content. Congress feared that the potential for liability would discourage investors from infusing capital to support the growth of these new companies, which were key players during this time of the Internet's infancy.[135] It hoped that treating websites as mere empty news racks for users to freely populate with content for the world to see would encourage these services to voluntarily self-police without the risk that a mistake would lead to civil liability.[136] *Zeran v. America Online, Incorporated*[137] expanded this immunity beyond publishers to distributors. In this case, a plaintiff sued AOL for not removing defamatory statements a third party posted about him.[138] But the Fourth Circuit worried about liability's chilling effect—it did not want AOL to restrict or censor posted content rigorously—so it extended Section 230 protection to distributors.[139]

As "one of the most valuable tools for protecting freedom of expression and innovation on the Internet,"[140] Section 230 likely precludes lawsuits where the website is the defendant. It has shielded Internet companies from liability in defamation, negligence, IIED, and privacy claims.[141] Therefore, victims cannot seek to make themselves whole from the likely least cost avoider with the deepest pockets.

Since suing the platforms seems to be a dead-end, plaintiffs should seek out those who created and those who distributed the DNCP, which may or may not be the same person. There is an argument that only the latter should be held liable, as it is the dissemination of the content that causes harm to the plaintiff. After all, one might argue that the mere isolated creation of DNCP does not result in harm to the victim who is

---

[134] *Id.* at *3.

[135] *See* 47 U.S.C. § 230(b) (2012) (five policy rationales behind Congress's enactment of Section 230).

[136] *See id.*

[137] 129 F.3d 327 (4th Cir. 1997).

[138] *Id.* at 330.

[139] *Id.* at 332.

[140] *Section 230 of the Communications Decency Act*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230 [https://perma.cc/7TKR-L8JL] (last visited July 31, 2022).

[141] *See, e.g.*, Batzel v. Smith, 333 F.3d 1018, 1020, 1026–27 (9th Cir. 2003) (defamation); Ben Ezra, Weinstein, & Co., Inc. v. Am. Online Inc., 206 F.3d 980, 983–84 (10th Cir. 2000) (defamation, negligence); Zeran v. Am. Online, Inc., 129 F.3d 327, 330, 332 (4th Cir. 1997) (negligence); Beyond Sys. v. Keynetics, Inc., 422 F. Supp. 2d 523, 525, 536 (D. Md. 2006) (Maryland Commercial Electronic Mail Act); Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 U.S. Dist. LEXIS 93348, at *2–3, 12–13 (E.D. Tex. Dec. 27, 2006) (negligence, intentional infliction of emotional distress, invasion of privacy); Barnes v. Yahoo!, Inc., No. 05-926-AA, 2005 U.S. Dist. LEXIS 28061, at *4, 11 (D. Or. Nov. 8, 2005) (negligence).

not aware of it. If the DNCP remains safely in the files of the creator, it does not traumatize anyone in real life and remains a victimless crime. But this position seems intuitively unsatisfying. Creating DNCP still feels wrong even if it is not shared. Plus, quantifying precisely how "bad" a certain act is seems like a line-drawing problem, capturing a difference in degree rather than in kind.

D. Intentional Infliction of Emotional Distress

Assuming the victim manages to identify a defendant and he is in the United States, tort remedies are adequate. However, because DNCP is an exercise of expression, the First Amendment complicates the analysis.

Intentional or reckless infliction of emotional distress ("IIED") appears most generally applicable to DNCP, though other torts are more suitable to certain narrow fact patterns. IIED is a catch-all tort meant to cover situations where an actor's conduct "exceeded all permissible bounds of a civilized society but an existing tort claim was unavailable."[142] All states have recognized IIED in some form.[143] The elements of an IIED tort are extreme and outrageous conduct that intentionally or recklessly causes severe emotional disturbance to another that results in emotional or bodily harm.[144] Unlike the related negligent infliction of emotional distress tort, physical injury is not a prerequisite for recovery.[145] With IIED, there is less risk of frivolous or outright bogus claims since the outrageousness of the actor's conduct is assurance that the emotional harm is real.[146]

Plaintiffs can successfully advance theories of IIED in court. For instance, an NCP plaintiff woman brings a lawsuit against her ex-boyfriend who had posted her nude images on twenty-three websites.[147] The court awarded her $425,000 in damages.[148] A more recent successful IIED claim, where the plaintiff sued an ex-boyfriend for posting sexual photos and videos of her, concluded with the court awarding the plaintiff $6.4 million in damages.[149]

---

[142] RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 46 cmt. a (AM. L. INST. 2012).

[143] *See* John J. Kircher, *The Four Faces of Tort Law: Liability for Emotional Harm*, 90 MARQ. L. REV. 789, 806 (2007).

[144] RESTATEMENT (SECOND) OF TORTS § 46 (AM. L. INST. 1965).

[145] 4A STUART M. SPEISER ET AL., THE AMERICAN LAW OF TORTS § 16:20 (2016).

[146] DAN B. DOBBS ET AL., THE LAW OF TORTS § 48 (2d ed.).

[147] Taylor v. Franko, No. 09-00002 JMS/RLP, 2011 WL 2746714, at *5 (D. Haw. July 12, 2011).

[148] *Id.* at *7.

[149] Christine Hauser, *$6.4 Million Judgment in Revenge Porn Case Is Among Largest Ever*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/us/revenge-porn-california.html [https://perma.cc/34K7-URLG].

Given these examples showing the strength of IIED in the NCP context, IIED is likely the most powerful tort available for DNCP victims. It is true that the presence of extreme and dangerous conduct might be difficult to prove in court, since images of various levels of nakedness are omnipresent in today's media.[150] But what is considered "extreme and dangerous conduct" is contextual and fact-sensitive, bending to society's expectations.[151] Courts have found certain extreme practical jokes and even words alone to be outrageous.[152] A DNCP plaintiff will likely successfully show that the actor's conduct was beyond the bounds of human decency, beyond what a civilized community would find tolerable.[153] Creating and circulating DNCP likely falls outside what reasonable minds think is acceptable behavior. [154] It violates privacy and ignites severe downstream consequences, which is likely more than enough to pass the "extreme and dangerous" bar.

Although the intent requirement is difficult to prove, the success of NCP IIED claims mentioned above is a testament to how this is not much of a challenge. Where the defendant is creating, sharing, or notifying the victim of the DNCP's existence, that voluntary act likely meets the requisite mens rea for the tort in spite of the defendant's likely claim that he did not mean to harm the victim.

Of course, the plaintiff will need to show distress severe enough to result in "mental suffering, mental anguish, mental or nervous shock, or the like."[155] One downside of this tort is that many courts do not find liability for purely emotional distress; thus, the harassment needs to escalate to the point where the victim manifests at least some bodily harm before she has a viable cause of action.[156] In other words, purely reputational or psychological harm is not enough to get into the court-

---

[150] *See generally* Jörg Matthes & M. Prieler, *Nudity of Male and Female Characters in Television Advertising Across 13 Countries*, 97(4) J. MASS COMMC'N Q. 1101 (2020).

[151] *See* RESTATEMENT (SECOND) OF TORTS § 46 cmt. d (AM. L. INST. 1965).

[152] *See* Daniel Zharkovsky, *"If Man Will Strike, Strike Through the Mask": Striking Through Section 230 Defenses Using the Tort of Intentional Infliction of Emotional Distress*, 44 COLUM. J.L. & SOC. PROBS. 193, 206 (2010).

[153] Harris, *supra* note 40, at 111.

[154] Danielle Citron and Robert Chesney argue that DNCP would count as outrageous conduct under IIED because it falls "outside the norms of decency." Chesney & Citron, *supra* note 1, at 1794.

[155] RESTATEMENT (SECOND) OF TORTS § 46 cmt. j (AM. L. INST. 1965).

[156] *See* 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, 257–58 (2015); Russell Fraker, *Reformulating Outrage: A Critical Analysis of the Problematic Tort of IIED*, 61 VAND. L. REV. 983, 1005–06 (2008).

house. But as we have seen from Ayyub's experience, the resulting humiliation and horror from DNCP can translate into bodily harm severe enough that no reasonable person should be expected to endure it.[157]

Due to free speech concerns, the actual malice standard may apply in the IIED context, depending on the plaintiff's status as a public figure. Under this standard, the defendant must have made the statement with "knowledge that it was false or with reckless disregard of whether it was false or not" to be held liable.[158] After Hustler Magazine published an article stating that famous minister Jerry Falwell's first sexual encounter was "a drunken incestuous rendezvous with his mother in an outhouse," Falwell sued the magazine for IIED.[159] However, because he was a public figure, he needed to show that Hustler Magazine made a false statement of fact with actual malice.[160] In the end, the Court reversed the Court of Appeals' holding for Falwell, finding that Falwell had failed to meet this burden.[161] The article was closer to a political cartoon or caricature, which are common tools of political debate that public figures should reasonably expect to come their way.[162]

For the DNCP creator defendant, actual malice with respect to the deepfake would be immediately met since the act of creation necessarily means the defendant has actual, personal knowledge of the final image's falsity. But the actual malice and mens rea analyses are murkier for a downstream DNCP distributor. Distributors might not expect the video they share with the public at large to ever reach the victim, meaning they will not think any emotional distress is eminent. However, this would not be the case if the distributor disseminates the video into a closed group he knows will bring the victim emotional distress, like a group comprised entirely of the victim's family. Although distributors may be remote from creation, their involvement in further circulating the DNCP arguably creates emotional distress as well.

1. The First Amendment

The biggest hurdle for an IIED plaintiff is undoubtedly the constitutional protection of free speech. Upholding the victim's privacy rights and upholding the actor's freedom of expression are in tension. In the course of developing First Amendment doctrine, the Supreme Court has maintained that restrictions on speech based on content are presumed

---

[157] Ayyub, *supra* note 65.

[158] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 280 (1964).

[159] Hustler Mag., Inc. v. Falwell, 485 U.S. 46, 48 (1988).

[160] *Id.* at 52.

[161] *Id.* at 56–57.

[162] *See id.* at 54.

invalid.[163] Disclosing and publishing NCP is seen as speech because it is "a communicative, symbolic act that expresses an idea,"[164] and this logic easily extends to DNCP. But nevertheless the "right to free speech is not absolute at all times and under all circumstances."[165] It leaves some categories of speech unprotected, such as obscenity, perjury, blackmail, and child pornography.[166]

What is absent from the list of unprotected categories of speech is falsity, because importantly falsity *alone* does not render something outside the bounds of First Amendment protection.[167] The Court has recognized that "[e]ven a false statement may be deemed to make a valuable contribution to public debate, since it brings about 'the clearer perception and livelier impression of truth, produced by its collision with error.'"[168] The marketplace of ideas concept provides the basis for protecting lies. There is no problem with false narratives circulating freely since vigorous discussion empowers people to discover which stories are actually true.[169] As the marketplace is adequate to correct pernicious opinions, the judicial system need not interfere.

2. Inapplicable Rationale

However, this theory of lies competing with truths until the latter prevails, justifying the constitutional protection of falsity, might not hold true online. Social media algorithms circulate deepfakes and other provocative content more readily than truthful, less attention-grabbing posts.[170] It is not truth that rises to the top, but what generates the most user engagement. In such situations, it is hard for the truth to compete. Plus, the majority of U.S. adults report they have trouble identifying whether information found online is trustworthy.[171] Even younger people, digital natives who grew up with technology and became proficient

---

[163] Ashcroft v. Am. C.L. Union, 542 U.S. 656, 665 (2004).

[164] *See* Sarah E. Driscoll, *Revenge Porn: Chivalry Prevails as Legislation Protects Damsels in Distress over Freedom of Speech*, 21 ROGER WILLIAMS U. L. REV. 75, 85 (2016).

[165] John A. Humbach, *The Constitution and Revenge Porn*, 35 PACE L. REV. 215, 220 (2014) (quoting Chaplinsky v. New Hampshire, 315 U.S. 568, 571 (1942)).

[166] Utset, *supra* note 71, at 943.

[167] United States v. Alvarez, 567 U.S. 709, 719 (2012) (plurality opinion).

[168] N.Y. Times v. Sullivan, 376 U.S. 245, 279 n.19 (quoting JOHN STUART MILL, ON LIBERTY AND OTHER ESSAYS 17 (Wiley-Blackwell 1947) (1859)).

[169] Robert D. Richards & Clay Calvert, *Counterspeech 2000: A New Look at the Old Remedy for "Bad" Speech*, 2000 B.Y.U. L. REV. 553, 585 (2000) (arguing that the best response to objectionable speech is counterspeech).

[170] *See* Filippo Menczer, *How "Engagement" Makes You Vulnerable to Manipulation and Misinformation on Social Media*, NIEMAN LAB (Sept. 13, 2021), https://www.niemanlab.org/2021/09/how-engagement-makes-you-vulnerable-to-manipulation-and-misinformation-on-social-media [https://perma.cc/4ACX-JV53].

[171] John B. Horrigan, *The Spectrum of Digital Readiness for E-learning*, PEW RSCH. CTR. (Sept.

with computers from an early age, find it difficult to confirm the authenticity of social media content.[172]

Further, this rationale of lies competing with truths is not as applicable to deepfakes, especially where they are so hyper-realistic "that the truth may never prevail unless there is some intervention, either through private website owners or by the government."[173] The victim circulating a statement asserting the image is a deepfake might be seen as attempting ex post damage control to salvage reputation rather than declaring the truth of the matter. All to say, DNCP does not lend itself to a prescription of counter-speech, which is an argument frequently employed to support First Amendment protection.[174] How does one counter the exposure of her intimate images? The depicted individual can attempt to announce that the image is fake, but the public has already been misinformed. Will the announcement even reach all who saw the image? Even if the announcement reaches them, will they believe it? The DNCP that will be the most difficult to debunk will be the ones that feed into confirmation bias.[175] If the depicted individual is already rumored to be provocative, then insisting on the image's falsity will be an uphill battle. Regardless of what the victim says in her defense, it will probably be futile since the ability to see something is uniquely convincing.

3. Lack of Matter of Public Concern

The First Amendment is likely a weak defense for IIED defendants because the First Amendment is primarily concerned with political speech and DNCP does not touch on matters of public concern. In *Snyder v. Phelps*,[176] the Court considered whether the First Amendment shielded the Westboro Baptist Church from liability for, among other claims, IIED.[177] The church believes that God hates the United States for tolerating homosexuality, including in its military.[178] In 2006, its members picketed outside a soldier's funeral with signs reading "Thank God for Dead Soldiers," "Priests Rape Boys," and "You're Going

20, 2016), https://www.pewinternet.org/2016/09/20/the-spectrum-of-digital-readiness-for-e-learning [https://perma.cc/C5CE-3VSM].

[172] Joel Breakstone, et al., *Evaluating Information: The Cornerstone of Civic Online Reasoning*, STAN. DIGIT. REPOSITORY (Nov. 22, 2016), http://purl.stanford.edu/fv751yt5934 [https://perma.cc/S2RB-4BAF].

[173] Wilkerson, *supra* note 19, at 418.

[174] Franks, *supra* note 54, at 1311.

[175] Brown, *supra* note 25, at 10.

[176] 562 U.S. 443 (2011).

[177] *Id.* at 450

[178] *Id.* at 448.

to Hell."[179] The soldier's father sued for IIED, and the jury found in his favor.[180] The Supreme Court, however, set aside the jury award, finding that the content of the church's speech related to matters of "political, social, or other concern to the community"[181] and not to matters of purely private concern.[182] Its messages touched on "the political and moral conduct of the United States and its citizens, the fate of our Nation, homosexuality in the military, and scandals involving the Catholic clergy."[183] Moreover, the church had notified authorities in advance of its plans to picket at the funeral and complied with police instructions in staging the demonstration.[184] Even if some of the speech was directed at the deceased, that "would not change the fact that the overall thrust and dominant theme of Westboro's demonstration spoke to broader public issues."[185] Applying the Court's logic to DNCP, it appears a plaintiff will be barred from recovery if a DNCP defendant is able to "couch [his] extreme and outrageous speech or conduct on the grounds of public concern."[186]

But while the Court reiterated its commitment to "uninhibited, robust, and wide-open" debates on public issues in *Snyder*,[187] it also opined that distributing a video of an employee engaged in sexual conduct is a private concern and thus less protected.[188] This kind of video "did nothing to inform the public about any aspect of the [employer's] functioning or operation."[189] DNCP of individuals engaged in a private act also does not inform the public about anything of public concern. And unlike the church demonstrators who sought some semblance of consent—albeit from local authorities and not from the affected plaintiff—DNCP creators and distributors are, by definition, not engaged in the same pre-approval.

If the public street where the church demonstrated is "the archetype of a traditional public forum" where free speech is traditionally exercised,[190] the Internet then is the archetype of a modern public forum in today's digital age. But there are limits to the public forum doctrine.

---

[179] *Id.*

[180] *Id.* at 447.

[181] *Id.* at 453 (quoting Connick v. Myers, 461 U.S. 138, 146 (1983)).

[182] *Id.* at 452.

[183] *Id.* at 454.

[184] *Id.* at 448–49.

[185] *Id.* at 454.

[186] Elizabeth M. Jaffe, *From the School Yard to Cyberspace: A Review of Bullying Liability*, 40 RUTGERS COMPUT. & TECH. L.J. 17, 31 (2014).

[187] *Snyder*, 562 U.S. at 452 (citing N.Y. Times v. Sullivan, 376 U.S. 254, 270 (1964)).

[188] *Id.* at 453 (citing San Diego v. Roe, 543 U.S. 77, 84 (2004)).

[189] *Id.* (quoting *San Diego*, 543 U.S. at 84).

[190] *Id.* at 456 (quoting Frisby v. Schultz, 487 U.S. 474, 480 (1988)).

Picketing on the public street around a particular residence or right outside an abortion clinic entrance without respecting a buffer zone are impermissible.[191] Similarly, DNCP creators and distributors can be understood as violating the private personal space of the victims.

The *Snyder* case is further distinguishable in that there was no pre-existing conflict between the parties to the lawsuit. Westboro had long been engaged in speaking on the subjects of its demonstration before it learned of Matthew Snyder.[192] Such circumstances mean it would be difficult to see how "Westboro's speech on public matters was intended to mask an attack on Snyder over a private matter."[193] But DNCP victims often do have pre-existing relationships with the actors. This is even more so the case for non-celebrities without images freely circulating online; actors would only be able to gather a faceset from the victim's private social media profiles.

E. Defamation

If IIED were to fail, an additional remedy could be found under defamation law. At common law, one's reputation has value.[194] Although the First Amendment liberally protects speech, the Court has held that "there is no constitutional value in false statements of fact."[195] The defamation tort imposes liability on those who make such false, public statements resulting in reputational harm.[196] Defamation by writing and analogous contemporary means is libel, whereas defamation communicated orally is slander.[197] Required elements include a false and defamatory statement about another, an unprivileged publication to a third party, fault of at least negligence on the actor's part, and harm from the publication.[198] Language is defamatory if it tends to expose the subject to shame, ridicule, degradation, or disgrace or induces "an evil opinion of [her] in the minds of right-thinking persons,

---

[191] *Id.* at 457.

[192] *Id.* at 455.

[193] *Id.*

[194] *See Leslie* Yolaf Garfield, *The Death of Slander*, 35 COLUM. J.L. & ARTS 17, 18 (2011) ("[In] the ecclesiastical courts of the middle ages . . . damning someone's reputation in the village square was worthy of pecuniary damage.").

[195] Gertz v. Robert Welch, Inc., 418 U.S. 323, 340 (1974). But later in United States v. Alvarez, the plurality opinion stated that false statements are not outside the protection of the First Amendment solely based on their falsity, so content-based restrictions should be "presumed invalid" unless those restrictions apply to certain categories of speech, such as defamation. 567 U.S. 709, 717 (2012).

[196] RESTATEMENT (SECOND) OF TORTS § 559 (AM. L. INST. 1977).

[197] DAN B. DOBBS ET AL., THE LAW OF TORTS § 519 (2d ed).

[198] RESTATEMENT (SECOND) OF TORTS § 558 (AM. L. INST. 1977).

and to deprive [her] of [her] friendly intercourse in society."[199] Publication is an act by which the defamatory matter is intentionally or negligently communicated to a third person.[200] The matter need not be made known to the public generally nor to a large group of persons.[201]

As with IIED, the proof required depends on whether the defamation plaintiff is a public figure. Public figures are persons "having some special prominence in the affairs of society or of the resolution of public questions."[202] Where the plaintiff is a public figure, she must bring evidence of actual malice—the actor made the statement "with knowledge that it was false or with reckless disregard of whether it was false or not."[203] Given their place in the public eye, they are regular targets of criticism, but not every attack is necessarily unlawful. In other words, the public figure plaintiff cannot recover for a defamatory falsehood unless she can show that the published statement was false and that the statement was made with the requisite mens rea.

Whether the plaintiff is required to prove "fault" on the part of the defendant depends on the content of the speech at issue too. If the plaintiff is suing for defamation from a statement on matters of public concern, the Supreme Court has indicated that "fault" is a necessary element to comply with free speech under the First Amendment.[204] Thus, many modern cases say that the defendant must be at least negligent to be found liable for defamation.[205] But where a private individual is suing for defamation from a published matter not of public concern, she need not show that the defendant was at fault nor bring evidence of actual loss to recover under the common law doctrine of presumed damages.[206]

DNCP constitutes a false and defamatory statement because (1) it is a doctored, and thus false, image that does not capture a real scene, and (2) the image where the identifiable victim appears to be naked or engaged in sexual activity is harmful to the victim's reputation. The average person probably thinks that only certain types of people would

---

[199] Celle v. Filipino Rep. Enterprises Inc., 209 F.3d 163, 177 (2d Cir. 2000).

[200] RESTATEMENT (SECOND) OF TORTS § 577 cmt. a (AM. L. INST. 1977).

[201] *Id.* at § 577 cmt. b.

[202] 8A SPEISER ET AL., THE AMERICAN LAW OF TORTS § 29:16 (2011).

[203] N.Y. Times Co. v. Sullivan, 376 U.S. at 280 (1964).

[204] Machleder v. Diaz, 538 F. Supp. 1364, 1371 (S.D.N.Y. 1982) ("In *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 [94 S.Ct. 2997, 41 L.Ed.2d 789] (1974), the Supreme Court held that the First Amendment to the Constitution does not permit the imposition of 'liability without fault' on 'a publisher or broadcaster of defamatory falsehood injurious to a private individual.'").

[205] DAN B. DOBBS ET AL., THE LAW OF TORTS § 519. (2d ed.).

[206] *Id.* at § 557. *See also* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985) (holding that in cases involving per se defamatory statements not involving matters of public concern, plaintiffs need not prove damages for fault for recovery.).

have such scandalous presence on the Internet such as adult entertainment stars and those with "bad" morals.[207] So at least for the average private individual, DNCP is creating a harmful and false statement about what kind of person the victim is.

Further, DNCP publication appears to satisfy the definition of defamation per se—it is a statement that imputes misconduct, lack of integrity, or inability in a person's trade, profession, or office.[208] With claims of defamation per se, the plaintiff is relieved from the burden of producing any proof that she has been injured.[209] Prima facie strict liability is appropriate because this form of defamation is "by [its] very nature . . . likely to cause mental and emotional distress, as well as injury to reputation, so there arguably is little reason to require proof for this kind of injury either."[210]

Tharpe v. Lawidjaja[211] shows how defamation could apply to DNCP. In that case, the plaintiff sued for defamation after the defendant altered—not with artificial intelligence but Photoshop—and distributed photos.[212] The photos depicted the plaintiff acting in a sexually explicit matter, identified the plaintiff as a "porn star," and attached identifiers to the photos linking them to the plaintiff's employer.[213] The court dismissed the defendant's motion for summary judgment, finding the statements to be defamatory per se.[214] The statements implied that the plaintiff was unfit to perform his job as a youth soccer coach and further prejudiced him in his profession.[215]

The fatal Achilles heel of bringing a defamation claim for DNCP is that the publication must be to a third party. There is no requisite publication, and thus no defamation claim, if the defamatory matter was communicated only to the person directly defamed.[216] This element means the tort will be underinclusive—it will leave out DNCP used privately for extortion or blackmail.

---

[207] Rana Ayyub explained that the DNCP campaign labeled her as "promiscuous" and "immoral." *See* Rana Ayyub, *In India, Journalists Face Slut-Shaming and Rape Threats*, N.Y. TIMES (May 22, 2018), https://www.nytimes.corn/2018/05/22/opinion/india-journalists-slut-shaming-rape.html [https://perma.cc/A7WR-PF6L].

[208] 50 AM. JUR. 2D LIBEL AND SLANDER § 141 (Aug. 2022).

[209] Gertz v. Robert Welch, Inc., 418 U.S. 323, 349 (1974).

[210] Carey v. Piphus, 435 U.S. 247, 262 (1978).

[211] 8 F. Supp. 3d 743 (W.D. Va. 2014).

[212] *Id.* at 751.

[213] *Id.* at 786.

[214] *Id.*

[215] *Id.*

[216] 8A SPEISER ET AL., AMERICAN LAW OF TORTS § 29:10 (2011).

F. Publicity in False Light

Closely related to the defamation tort is the publicity in false light tort. In fact, defamation and false light are often brought together. The damage to the victim's reputation is the basis for the defamation claim, while mental distress from exposure to public view is the basis for the publicity in false light claim.[217] Publicity in false light protects one's peace of mind.[218] An actor who gives publicity to a matter concerning another that places the other in a false light is liable if the false light would be "highly offensive to a reasonable person" and "the actor had knowledge of or acted recklessly as to falsity of the publicized matter and the false light in which the other would be placed."[219] Unlike defamation, the publicized matter for false light only needs to be false, not false *and* defamatory.[220] In this way, false light's lower threshold means greater chances for a plaintiff to prevail.

Unlike defamation, which assigns different plaintiffs different burdens of proof, false light requires that all plaintiffs, whether public or private figures, prove actual malice on the part of the defendant.[221] However, this requirement will not doom DNCP cases where the defendant is the creator. Since the original act of generating the doctored image indicates knowledge of the publicized matter's falsity, suits against creators of DNCP would likely meet this element. Where the defendant is a DNCP distributor, actual malice would be a more formidable hurdle.

Whereas "publication" in defamation is satisfied with an unprivileged transmission to a single third party, "publicity" in false light is a high bar. To pass this bar, the information must be either shared with the public at large or to "so many persons that the matter must be substantially certain to become public knowledge."[222] This requirement may be hard to meet in cases where the DNCP is shared with a limited group or to niche websites.

There are, however, compelling policy reasons for why courts should consider loosening the "widely shared" requirement. Although a strict rule prevents frivolous litigation, it seems arbitrary to presume that sufficient harm to find the defendant liable only manifests when

---

[217] *Id.* § 29:3.

[218] Romaine v. Kallinger, 537 A.2d 284, 294 (N.J. 1988) (quoting RESTATEMENT (SECOND) OF TORTS § 652E cmt. b (1977)).

[219] RESTATEMENT (SECOND) OF TORTS § 652E (AM. L. INST. 1965).

[220] Russell Donaldson, Annotation, *§ 8. Nondefamatory False Light as Actionable*, 57 A.L.R. 4th 22.

[221] 9 SPEISER ET AL., AMERICAN LAW OF TORTS § 30:32 (2012) (Colorado, Florida, North Carolina, Texas, and Ohio do not recognize the tort of false light).

[222] RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (AM. L. INST. 1965).

the disclosure is made to a wide audience. DNCP shared with a small group of people, where its members have influence over the plaintiff's life, is just as damaging. Moreover, in terms of administrability, broadening this standard would remove the demanding inquiry of determining how much exposure is enough for public disclosure.

It seems natural to apply false light to DNCP. The tort comes from "an awareness that people who are made to seem pathetic or ridiculous may be shunned, and not just people who are thought to be dishonest or incompetent or immoral."[223] In *Douglass v. Hustler Mag., Inc.*,[224] the plaintiff sued for publicity in false light after the magazine published nude photos she had taken for a different magazine. She argued that Hustler's publicity insinuated she was a lesbian and the kind of person who would be willing to be shown naked in the defendant magazine.[225] The Seventh Circuit concluded that this was enough for the plaintiff to have a cause of action for false light.[226] Just as it would be reasonable for a jury to find the plaintiff's association with the magazine as degrading and offensive, it is reasonable for a DNCP victim whose likeness is shared on an escort or prostitute services website to claim that the association is degrading and offensive.[227]

The plaintiff in *Lerman v. Flynt Distrib. Co.*[228] was misidentified as the woman in a nude photograph in a magazine.[229] The Second Circuit conducted a false light analysis and concluded that the publicity given to a photo of a nude actress who was not actually the plaintiff satisfies the "highly offensive to a reasonable person" standard.[230] This logic extends to DNCP too, as DNCP depicts a person who is not exactly of the plaintiff herself either.

Because false light involves communication, this tort implicates free speech concerns. In the case where there is a disclaimer as to the content's falsity, a court balancing the defendant's First Amendment rights to create fictitious works against the plaintiff's privacy rights may side with the defendant. But letting a disclaimer function as a get-out-of-liability card for the defendant might sweep too broadly. Even with these disclaimers, a court should still consider the possibility that the downstream viewer may not see the disclaimer if it were edited out altogether.

---

[223] Douglass v. Hustler Mag., Inc., 769 F.2d 1128, 1134 (7th Cir. 1985).

[224] *Id.*

[225] *Id.* at 1135.

[226] *Id.* at 1138.

[227] *Id.*

[228] 745 F.2d 123 (2d Cir. 1984).

[229] *Id.* at 134–35.

[230] *Id.* at 136.

G. Intrusion on Seclusion

Intrusion on seclusion protects the right to be let alone.[231] This tort is available to plaintiffs whose private place or affairs were intentionally invaded, physically or otherwise, in a way that a reasonable person would find "offensive and objectionable."[232] Despite this seemingly broad formulation, most courts require some sort of invasion into a physical space.[233]

The information taken by the actor during the intrusion need not be communicated to a third party for the plaintiff to have a claim, so DNCP creators who do not publish are potentially liable.[234] Additionally, because the nature of this tort is intrusion, which is more conduct-like, and not publication, which is more speech-like, finding the defendant liable is less likely to raise the same level of First Amendment concerns as the other torts discussed.[235]

DNCP's artificiality is not an obstacle since this tort does not hinge on the truth or falsehood of the information but rather on how the actor obtained it.[236] However, the physical intrusion requirement may pose an issue, as courts are unlikely to find that the DNCP creator pulling input data already circulating online, the typical process of gathering a faceset, to be physical intrusion into a private space. In these situations, there was no actual violation of the victim's personal space. Media posted on the Internet, whether voluntarily by a private individual or by journalists documenting public figures, cannot be reasonably expected to remain private.[237] NCP is more like an actual invasion, whereas DNCP is only the *appearance* of an invasion.

But perhaps the mere appearance of invasion should be sufficient to give rise to a cause of action. The risk of frivolous DNCP lawsuits is low given litigation-related burdens on the plaintiff, so there is less need for the judicially created physical intrusion requirement to serve as a limiting principle.[238] From the average observer's perspective, DNCP seems objectively intrusive. And from the victim's perspective,

---

[231] 9 SPEISER ET AL., AMERICAN LAW OF TORTS § 30:09 (2012).

[232] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 395–96 (1960).

[233] Welsh v. Martinez, 114 A.3d 1231 (Conn. App. Ct. 2015) (defendant placed spying devices in the plaintiff's bedroom); In re Marriage of Tigges, 758 N.W.2d 824, 829 (Iowa 2008) (defendant surreptitiously filmed plaintiff in their shared home); Lewis v. LeGrow, 670 N.W.2d 675 (Mich. Ct. App. 2003) (defendant secretly filmed plaintiff and him having sex).

[234] 9 SPEISER ET AL., AMERICAN LAW OF TORTS § 30:09 (2012).

[235] DAN B.DOBBS ET AL., THE LAW OF TORTS § 580 (2d ed.).

[236] Trundle v. Homeside Lending, Inc., 162 F. Supp. 2d 396, 401 (D. Md. 2001).

[237] *See* Anne Pechenik Gieseke, *"The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography*, 73 VAND. L. REV. 1479, 1497 (2020).

[238] Legal action remains rare for victims of online harassment. Citron, *supra* note 62, at 23–24.

she is not any less harmed if the photos were downloaded without her consent from her social media profile than if they were taken secretly with bugged cameras in her home. She expects a certain degree of privacy and protection in both settings.

Although the specific facts of each DNCP case will vary, there is, thankfully, a menu of potential tort remedies. While IIED may have the broadest reach, in other instances defamation, publicity in false light, or intrusion on seclusion may be a better fit.

IV. CONCLUSION

DNCP's dangers stem from its generation of a new reality. This fabricated reality is a disease, not only harming the victim's sense of identity but infecting her relationships with others as well. And as with illness, prevention of DNCP is better than a cure. No matter the criminal sentence or civil damages award, the harm would have already occurred. It may be compensable, but it is irreversible.

While we wait for criminal laws to catch up with the technological times, victims need not helplessly sit around. There already exists a suite of tort solutions that can be used to fight back against the absolute dystopian nightmare that is DNCP.