Reframing Deepfakes

Jennifer E. Rothman*

* Jennifer E. Rothman is the Nicholas F. Gallicchio Professor of Law at the University of Pennsylvania Carey Law School. This essay is adapted from a lecture given at Columbia Law School on October 24, 2025, at the Symposium *Deepfakes: In Search of Global Solutions*, co-sponsored by Columbia Law School's Kernochan Center and the Columbia-Sorbonne Alliance. I am thankful for comments from Sarah Boyd, Jane Ginsburg, Michael Goodyear, Jacob Noti-Victor, Elizabeth Pollman, the participants and organizers of the Symposium, and the journal editors, as well as research assistance from Penn Carey Law's library staff, particularly the excellent work by Genevieve Tung, as well as additional research assistance by Rachel Buckland and Shivani Chelliah.

INTRODUCTION

The circulation of deceptive fakes of real people appearing to say and do things that they never did has been made ever easier and more convincing by improved and still improving technology, including (but not limited to) uses of generative artificial intelligence ("AI"). I was asked to speak about the legal landscape in the United States that regulates deepfakes, as well as some predictions of what may be on the horizon in terms of potential future legislation. In some sense, this is a nearly impossible task as hundreds of laws have passed in just the last few years to address concerns over deepfakes. California, for example, seems to be passing new AI-related laws almost every week; six laws were passed in just the last three weeks.[1] So, instead of trying to

1. A.B. 325, 2025 Gen. Assemb., Reg. Sess. (Cal. 2025) (limiting uses of common pricing algorithms); A.B. 489, 2025 Gen. Assemb., Reg. Sess. (Cal. 2025) (regulating undisclosed use of AI tools in healthcare to imply provision of care by "natural person"); S.B. 243, 2025 Gen. Assemb., Reg. Sess. (Cal. 2025) (regulating AI companion chatbots); A.B. 853, 2025 Gen. Assemb., Reg. Sess. (Cal. 2025) (expanding transparency requirements for AI platforms and delaying implementation date of prior transparency provisions); A.B. 621, 2025 Gen. Assemb., Reg. Sess. (Cal. 2025) (expanding prohibition on deepfake pornography); A.B. 316, 2025 Gen. Assemb., Reg. Sess. (Cal. 2025) (preventing civil defendants from avoiding liability by claiming harm was caused by AI tools acting "autonomously"); Kara Williams & Mayu Tobin-Miyaji, *California Tech Legislation Roundup: Numerous Privacy and AI Laws Enacted and Six Vetoed*, EPIC.ORG (Oct. 15, 2025), https://epic.org/california-tech-legislation-roundup-numerous-privacy-and-ai-laws-enacted-and-six-vetoed/ [http://web.archive.org/web/20260206202511/https://epic.org/california-tech-legislation-roundup-numerous-privacy-and-ai-laws-enacted-and-six-vetoed/]. Several of these new bills have particular relevance for deepfakes, including requirements of transparency tools to detect and disclose AI, increasing statutory damages for deepfake pornography, and limiting defenses for AI developers and users.

cover everything, I want to set forth some guideposts for sorting through this increasingly complicated landscape, and only then consider the existing laws that cover identity rights and that likely or explicitly apply to deepfakes, including digital replicas, forgeries, and voice clones.[2] I will also consider some new legislation being contemplated, particularly at the federal level.

As part of these guideposts, I will propose a taxonomy of deepfakes that should guide our understanding of this area of law. Before developing this taxonomy, I will start in Part I by providing a foundational understanding of what we mean by the term "deepfakes," and then in Part II highlight the reasons why we are concerned about them. Both steps are essential before I can construct the taxonomy in Part III.

Developing the proposed taxonomy of deepfakes is a desperately needed task as the urgent calls for legislative fixes to address deepfakes have collapsed distinct types of fakes into one single monolith. This lack of nuance when speaking about deepfakes has sometimes masked the problems at issue and obscured the applicability of existing legal structures to combat them. I divide deepfakes (of humans) into four categories: *unauthorized*; *authorized*; *deceptively-authorized*; and *fictional*. As part of this analysis, I identify the two key considerations for regulating deepfakes, which are (1) whether the fakes are *authorized* by the people depicted in them and (2) whether the fakes *deceive the public* into thinking they are authentic recordings.

In Part IV, I use this taxonomy of deepfakes and our understanding of the harms that potentially flow from each type of deepfake to evaluate whether current and proposed laws address our concerns, exacerbate them, or create new challenges. Unfortunately, much of the recently proposed and enacted legislation does not adequately focus on limiting deceptive deepfakes, and in some instances even legitimizes and incentivizes the creation of them.

I. DEFINING DEEPFAKES

It may seem strange to start by defining the very topic of the symposium. Nevertheless, understanding the scope of what is covered by the term is an essential first step in considering the role of current (and proposed) laws. We must have a sufficiently specific and common definition so we can understand the boundaries of the term and consider whether deepfakes are something substantively new or simply a new manifestation of something longstanding.

The term "deepfakes" is thought to have originated in 2017 with a Reddit user who went by that name and used the term to refer to pornographic images that swapped in the faces of real people to the bodies of others to make it seem like those whose faces were depicted had appeared in the intimate and explicit situations shown when they had not.[3] Since 2017 both the use of the term and its meaning have exponentially

2. I will develop further the meaning of these terms in Part I.

3. Meredith Somers, *Deepfakes, Explained*, MIT SLOAN SCH. MGMT. (July 21, 2020), https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained? [http://web.archive.org/web/20260206203122/https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained] (defining a deepfake as "a specific kind of synthetic media where a person in an image or video is

grown.[4] What was once thought to be primarily a nonconsensual pornography problem has expanded to encompass difficult-to-detect video and voice fakes that simulate or impersonate people in any context. Congressional representatives and some state legislatures have used the language of "digital forgeries" of "identifiable individual[s]" to capture the concept of deepfakes.[5] Some state laws and proposed federal ones, along with the U.S. Copyright Office, have instead adopted the term "digital replicas" and "voice clones" to refer to deepfakes.[6]

The definitions of digital replicas themselves vary. For example, the proposed NO FAKES Act, introduced in April of 2025 in both the U.S. House and Senate, defines a "digital replica" as a "newly-created, computer-generated, highly realistic electronic representation that is readily identifiable as the voice or visual likeness of an

swapped with another person's likeness" and tracing the term's origin to 2017 Reddit user "deepfake"). The Reddit user likely also adopted the term in reference to the "deep" learning technique used by artificial intelligence. *See Deepfake*, ENCYC. BRITANNICA (Feb. 4, 2026), https://www.britannica.com/technology/deepfake [http://web.archive.org/web/20260206203414/https://www.britannica.com/technology/deepfake] (noting that "[t]he term *deepfake* combines *deep*, taken from AI deep-learning technology (a type of machine learning that involves multiple levels of processing), and *fake*, addressing that the content is not real").

4. Although I note that a recent Uniform Law Commission drafting committee narrowed its focus to deepfakes only in the pornographic context after forming a study committee to consider deepfakes more broadly. *Compare* SUZANNE BROWN WALSH & EUGENE VOLOKH, DEEPFAKES STUDY COMM., FINAL STUDY COMMITTEE REPORT 2 (2024), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=f0b236e5-f8b6-1825-d0c7-baa88e08256b&forceDialog=0; (considering both election-related deepfakes and those with sexual content), *with* Memorandum from Eugene Volokh to Drafting Comm. on Nonconsensual Pornographic Deepfakes 4 (Dec. 6, 2024) (limiting scope of drafting to uniform law addressing "nonconsensual pornography"), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=fd4a4157-1d1c-efce-ceb3-688a6e048b9d&forceDialog=1 .

5. The proposed DEFIANCE Act of 2024 focused on "sexually-explicit 'deepfakes,'" describing them as a "digital forgery," "created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means" to falsely appear to be authentic." DEFIANCE Act of 2024, S. 3696, 118th Cong. § 3(a) (2024); *see also* 18 PA. CONS. STAT. § 4101.1 (2025) (creating crime to produce non-consensual "forged digital likenesses," including deepfakes and voice clones, defined as "a computer-generated visual representation of an actual and identifiable individual or audio recording of an actual and identifiable individual's voice"); *see also* Bobby Chesney & Danielle K. Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1758 (2019) (describing "deep fakes" as a form of "realistic and convincing" "digital impersonation").

6. *See, e.g.*, NO FAKES Act of 2025, S.1367, 119th Cong. § 2(a) (introduced Apr. 9, 2025); U.S. COPYRIGHT OFF., COPYRIGHT AND ARTIFICIAL INTELLIGENCE: PART I: DIGITAL REPLICAS (July 2024); *see also* Preventing Abuse of Digital Replicas Act (PADRA), 118th Cong. (Discussion Draft as introduced by Rep. Darrell Issa, Aug. 9, 2024) (defining a digital replica as a "a computer generated, electronic representation of an identifying characteristic of a subject person, who is an individual human being" but limiting to instances in which the "identifying characteristic" is "distinctive to said subject person" and will be so "associated" with them by reasonable persons in the "relevant industry or market" that the representation is "substantially indistinguishable" and would be "apparent" that "was generated . . . to duplicate" the person (or the identifiable characteristic)).

individual."[7] The Copyright Office defines a digital replica more broadly as "the use of digital technology to realistically replicate an individual's voice or appearance."[8]

The FBI has defined deepfakes as encompassing "a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said."[9] *Merriam-Webster's Dictionary* has adopted a similar definition of a deepfake as "an image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said."[10]

Although there are many similarities across these (and other) definitions of deepfakes, there are also significant differences. I want to highlight two crucial ones. First, the definitions differ in whether a deepfake must deceive or be likely to deceive the public that it is an authentic recording or instead simply needs to depict an identifiable person regardless of deception.[11] Some definitions add a requirement that the actor/potential defendant intended to deceive the public by creating or disseminating the deepfake.[12] The requirement of intent to deceive may be driven by concerns that a strict liability or even negligence standard may violate the First Amendment, especially in the context of criminal charges.[13]

A second major difference among the definitions of deepfakes is whether the term only applies to depictions of people or also applies to depictions of objects and places. The European Union's AI Act has adopted a broader vision of deepfakes, as including

---

7. NO FAKES Act of 2025, *supra* note 6, at § 2(a).

8. U.S. COPYRIGHT OFF., *supra* note 6, at "About This Report."

9. *Public Service Announcement: Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions,* FBI INTERNET CRIME COMPLAINT CTR. (IC3) (June 28, 2022), https://www.ic3.gov/PSA/2022/PSA220628 [https://perma.cc/YGA6-PPYY].

10. "*Deepfake*," MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/deepfake [http://web.archive.org/web/20260206231320/https://www.merriam-webster.com/dictionary/deepfake] (last visited Feb. 8, 2026).

11. *Compare* 18 PA. C.S.A. § 4101.1(f)(3) (defining a "forged digital likeness" for purposes of a criminal offense as "a computer-generated visual representation" of a person that "is likely to deceive a reasonable person to believe that the visual representation or audio recording is genuine") *and* WASH. REV. CODE § 42.62.020 (2026) (limiting use of "synthetic media" in political campaigns only if a "reasonable individual" would believe such media to depict a real "appearance, action, or speech"), *with* CAL. CIV. CODE § 1708.86 (2026) (realistic intimate image need not deceive the viewer into thinking depicts real events or authorization by person depicted), *and* TENN. CODE ANN. § 47-25-1103 (Elvis Act of 2024) (tying liability for circulation of digital replicas to their authorization not whether they deceive the public). Notably, New York's postmortem right of publicity statute used to limit liability for uses of digital replicas to those that were "likely to deceive the public" but removed this limitation in late 2025, expanding liability to nondeceptive uses. *See* 2025 N.Y. Laws ch. 616 (S.8391) (signed into law Dec. 11, 2025).

12. *See, e.g.*, TEX. ELEC. CODE § 255.004(e) (2019) (defining deep fake videos as ones that with "intent to deceive . . . appear[] to depict a real person performing an action that did not occur in reality"); TEX. PEN. CODE § 21.165 (2024) (same in context of sexually-explicit content); S.B. 1515, 56th Leg., 2d Reg. Sess. (Ariz. 2024) (proposing election-related regulation of deepfakes that would require intent to harm reputation of person depicted or deceive voters).

13. *Cf.* Counterman v. Colorado, 600 U.S. 66 (2023) (holding that criminal liability for speech requires at least recklessness standard in context of true threats); *Ex parte* Jones, No. PD-0552-18, 2021 WL 2126172 (Tex. Ct. Crim. App. 2021) (reading in narrowing construction of intimate image law in Texas so that requires that person who circulated the image knew or was reckless as to lack of consent).

depictions of "objects, places, entities [and] events" as well as of people.[14] The *Encyclopedia Britannica* also takes this approach and does not limit deepfakes to those that depict human beings.[15]

For purposes of this Lecture, I am going to focus on deepfakes of people rather than those of objects or places both because this has been the focus of concern and legislation in the U.S. and also because we have hundreds of years of various laws that focus on unauthorized uses of a person's identity, particularly their names and likenesses, that apply or may apply to such uses in the context of deepfakes.

I also adopt a definition of deepfakes that does not require demonstration that a viewer or listener has been deceived. The deepfake must appear to be an authentic recording of the person depicted but need not do so deceptively. Nor does appearing authentic require that the alleged recording seem realistic or be in a realistic context.

With these central determinations, my operative definition of a deepfake is: "An image, sound, or performance that depicts a person and appears to be an authentic recording of that person when it is not one." Note that I use "depict" here to encompass both use of a person's likeness and their voice.[16] In spite of the etymological origins of the verb "to depict" to indicate visual depictions, there is no alternative word that captures the meaning as well for audio depictions so I use the term to mean both. In addition, note that this definition includes deepfakes made using any technology, whether computer-generated or not, and without regard to whether AI is used. There is variation across definitions on this point too, but I think the best approach is to be technologically neutral.

I am not suggesting that we adopt this definition formally or write it into legislation. Instead, I view the definition as a starting point that we may wish to further refine. I also am not committed to the terminology "deepfake" but it is a term frequently employed and is the chosen term for this symposium. And if a deepfake is understood as a more neutral term than it sometimes is, it has some advantages conceptually over "digital replicas," "voice clones," or "digital forgeries." Deepfakes can be understood as encompassing a wider variety of uses than these targeted, alternative terms, including uses that are not digital, and that are not rooted to a particular context, like the entertainment industry, or a particular legal frame, like criminal conduct.

Having a working definition of deepfakes is essential for understanding and teasing apart the different types of deepfakes that so often have been either conflated or insufficiently distinguished. Before undertaking that task, however, I want to briefly sketch out some of the harms that flow from deepfakes that depict people.

---

14. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, Laying Down Harmonised Rules on Artificial Intelligence, art. 3(60) 2024 O.J. (L 1689) 1 [EU AI Act]. The Uniform Law Commission (ULC)'s recent Study Committee on Deepfakes initially also took such a broad approach defining "'deepfakes' as shorthand . . . to refer to all video, photographic, and audio forgeries." FINAL STUDY COMMITTEE REPORT, *supra* note 4, at 2.

15. *See Deepfake*, *supra* note 3.

16. Likeness, if interpreted broadly to be a representation of a person's identity, could include voice, but it is useful to separate them for clarity as likeness is most often understood as pointing to a person's visual features.

II. HARMS OF DEEPFAKES

I suspect that the harms created by deepfakes are familiar to this audience. They are nevertheless important to remind ourselves of because, particularly in the United States, sometimes these concerns get lost when drafting legislation with a focus on generating or protecting income for particular industries, such as the recording industry, internet platforms, or technology companies. Failure to know what problems we seek to address makes it impossible to evaluate the sufficiency of the already existing legal frameworks.

In addition, although deepfakes is a term that is most often used pejoratively, not all deepfakes should be prohibited or subjects of legal liability. Distinguishing between when the law should step in and when it should step back in the context of deepfakes requires a more nuanced understanding of what harms flow from the dissemination of some (but not all) deepfakes.

There are three main categories of harms that flow from the dissemination of deepfakes: (a) ones that negatively impact the individuals depicted; (b) those that cause broader harms to the public, particularly by deceiving the public into thinking the fakes are real; and (c) those that negatively affect either those close to the person depicted or those with financial interests entangled with the person depicted. Not all of these harms deserve legal redress but those that do largely arise in two main contexts: (1) when they are *not authorized* by the person depicted; or (2) when they *deceive the public* as to their authenticity.

Sometimes deepfakes are both unauthorized and deceptive and at other times they may be one without the other. In each of these instances, some harms are likely to flow. I will largely focus on the harm to living people but will note when relevant issues are raised by deepfakes that portray the deceased.[17] If a deepfake is authorized and not deceptive, it is presumptively benign; even though such fakes may lead to market disruption, these harms are generally not appropriate for legal remediation.

A. HARMS TO PERSON DEPICTED

Unauthorized deepfakes, like other unauthorized uses of a person's identity, can cause a host of personal and economic injuries to the person depicted.[18] Losing control over one's own name, image, likeness, and voice harms our right of self-determination and autonomy. There is a longstanding understanding that we each have both liberty-based and property-based rights in our own names, likenesses, and identity more

17. I note that I use the term "portray" to include both audio and visual depictions, even though the word "portray," like "depict," stems etymologically from a visual context.

18. JENNIFER E. ROTHMAN, THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD 98–112 (2018) (considering and evaluating various justifications for protections against unauthorized uses of a person's identity); Robert C. Post & Jennifer E. Rothman, *The First Amendment and the Right(s) of Publicity*, 130 YALE L.J. 86, 93–125 (2020).

broadly.[19] Unauthorized deepfakes may also cause humiliation and degradation that injures a person's dignity and reputation. This is particularly so when a person is placed in troubling contexts, such as pornography or saying problematic or offensive things that they never said.[20] This harm exists even if the use does not deceive the public as to its authenticity, though the scale of the harms may differ.[21]

The person depicted may also suffer a range of market-based harms from "lost job opportunities and endorsement deals to reduced salaries, loss of revenue from licensing and merchandising contracts, and overall diminishment of [their] goodwill."[22] This is particularly true (but not exclusively so) for those who actively commercialize their identities. Unauthorized deepfakes, particularly of performances, could substitute for hiring the person themselves and, if not regulated, could reduce incentives for actors, singers, and other performers to create such performances in the first place.[23]

In the context of deceased individuals who are depicted in deepfakes, they can no longer suffer direct personal injuries. Nevertheless, we might consider injuries to the living (what I elsewhere refer to as "future-decedents") who may be troubled by their own potential postmortem treatment in deepfakes. The consideration of postmortem identity rights and deepfakes that depict the deceased is a large topic unto itself and one that I cannot do justice to here, but one that I have considered in depth elsewhere.[24]

---

19. *See* Vidal v. Elster, 602 U.S. 286 (2024) (considering long history of protecting a person's name under trademark and unfair competition laws); Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68, 76–77 (Ga. 1905) (concluding that rights over a person's likeness is both a liberty and property right); Roberson v. Rochester Folding Box Co., 64 N.E. 442, 449–50 (N.Y. 1902) (Gray, J., dissenting) (suggesting that every person has a "property right" in their own "person" and image); Corliss v. E.W. Walker Co., 64 F. 280, 282 (C.C.D. Mass. 1894) (recognizing that every person has a property right in their portrait); ROTHMAN, *supra* note 18, at 11–44; Jennifer E. Rothman, *Navigating the Identity Thicket: Trademark's Lost Theory of Personality, the Right of Publicity, and Preemption*, 135 HARV. L. REV. 1271, 1297 (2022); *The Right to Privacy*, 6 GREEN BAG 498, 499 (1894) (suggesting that there is "a right of property in one's personal appearance"); *see also* Anita L. Allen & Jennifer E. Rothman, *Postmortem Privacy*, 123 MICH. L. REV. 285, 297–98, n.53 (2024) (considering framing of publicity and privacy rights arising out of a person's identity as a property right in context of postmortem privacy).

20. *See* Post & Rothman, *supra* note 18, at 121–25, 165–71; *see also* Chesney & Citron, *supra* note 5, at 1771–75 (pointing to harms from deepfakes arising from extortion, sexual "exploitation," and "sabotage"); Michael P. Goodyear, *Dignity and Deepfakes*, 57 ARIZ. ST. L.J. 931, 942–53 (2026) (focusing on dignitary injuries caused by being portrayed in deepfakes, particularly though not exclusively in the context of sexualized depictions). Some states have extended postmortem rights targeting depictions of soldiers specifically to preserve the dignity of the deceased and their surviving relatives. *See, e.g.*, ARIZ. REV. STAT. § 12-761; ARIZ. REV. STAT. § 13-3726; LA. REV. STAT. ANN. § 14:102.21; *see also* Allen & Rothman, *supra* note 19, at 318–20, 322–24 (considering dignity-based reasons for protecting postmortem rights).

21. *See* discussion *infra* Part III.A.

22. Post & Rothman, *supra* note 18, at 108 (citing WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 222–28 (2003); ROTHMAN, *supra* note 18, at 110–11; Mark F. Grady, *A Positive Economic Theory of the Right of Publicity*, 1 UCLA ENT. L. REV. 97, 103–04 (1994)).

23. This is particularly relevant when the underlying performance is not protected by copyright. *See, e.g.*, Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562 (1977). In such instances, the objectives of identity rights and copyright law overlap. *See id.* at 575; Post & Rothman, *supra* note 18, at 96–106.

24. *See* Allen & Rothman, *supra* note 19, *passim* (considering a variety of interests that could support postmortem publicity rights, including the interests of "future-decedents," the "relational-living," and of society more generally); *see also* ROTHMAN, *supra* note 18, at 81–86 (considering expansion of right of publicity laws to cover postmortem rights); Jennifer E. Rothman, *Postmortem Publicity Rights at the Property-Personality*

B. HARMS TO THE PUBLIC

Deceptive deepfakes—whether authorized or not by the person depicted—also can cause significant harm to the public. They can destabilize our political system by circulating fake images and recordings of political figures saying and doing things they never did in ways that can affect how voters perceive them and alter the outcome of elections. Deepfakes of politicians could cause civil unrest and even global catastrophes by inciting wars or conflicts engendered by false statements or actions appearing to be authentic speech or conduct by a world leader.[25]

Deceptive deepfakes can also more broadly destabilize our access to information and truth. As Brian Chen recently wrote in the *New York Times*, we may be facing the "end of visual fact."[26] Can society survive if we not only do not have common references and sources, but also do not have reliable documentation of real-world events? The criminal justice system and the tort system will themselves be threatened by the undermining of image-and-voice-based evidence.[27]

We as a society may also be impoverished by AI-generated slop in the place of high-quality content. This could happen with nondeceptive deepfakes too, but as long as the public is able to knowingly choose between deepfakes and authentic performances this is not something the law should generally attend to when the uses are otherwise authorized.[28] But it is reasonable to construct a legal regime that supports the public knowingly choosing to watch AI-generated performances rather than consuming them thinking they are watching or listening to real actors and singers.[29]

Deceptive deepfakes can also disrupt consumer markets, leading people to make purchasing decisions based on false information about what a depicted person endorses or uses.

Divide, *in* PRIVATE LAW THEORY & INTELLECTUAL PROPERTY (Shyamkrishna Balganesh, Poorna Mysoor & Henry Smith eds., Cambridge Univ. Press forthcoming 2027), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4971180 (suggesting that if we conceptualize the right of publicity as a property right, then its unique status indicates that any postmortem right is best understood as something new rather than as a descendible right).

25. For a useful analysis of some of these harms, *see* Chesney & Citron, *supra* note 5, at 1771–86.

26. Brian X. Chen, *A.I. Video Generators Are Now So Good You Can No Longer Trust Your Eyes*, N.Y. TIMES, Oct. 9, 2025, https://www.nytimes.com/2025/10/09/technology/personaltech/sora-ai-video-impact.html [https://web.archive.org/web/20251009113425/https://www.nytimes.com/2025/10/09/technology/personaltech/sora-ai-video-impact.html].

27. *See* Rebecca A. Delfino, *Deepfakes on Trial: A Call to Expand the Trial Judge's Gatekeeping Role to Protect Legal Proceedings from Technological Fakery*, 74 HASTINGS L.J. 293, 297 (2023).

28. Such authorization may need to include authorization by copyright holders, as well as by the person(s) depicted. AI outputs may infringe copyrighted works and it is an open question of whether training AI models using copyrighted materials and people's identities is infringing of copyrights and publicity rights. *See infra* note 70 and accompanying text.

29. *See* Jacob Noti-Victor, *Regulating Hidden AI Authorship*, 111 VA. L. REV. 139 (2025).

C. HARMS TO RELATED PARTIES

Those close to those depicted may also suffer emotional distress, such as a parent seeing their child depicted in deepfake pornography, or a relative seeing their deceased loved one reanimated against their wishes. Unauthorized deepfakes could also disrupt the income for companies that have invested in a person's performance or that hold the copyrights to various works in which the person appears that may have been used to create the deepfakes. This is particularly a risk when the fakes might substitute for paying for authentic works by the underlying person.

* * *

This overview of the harms that flow from deepfakes highlights that the key determinants of whether deepfakes cause harm stem from whether the deepfakes are *unauthorized* or *deceptive* or both. This focus informs the development of the taxonomy that follows.

III. A TAXONOMY OF DEEPFAKES

To the extent deepfakes are distinguished from one another it has primarily been on the basis of the context in which the fakes appear—for example, to distinguish among deepfakes that appear in the context of political campaigns or that depict politicians, those that show private body parts or are otherwise pornographic, and those that impersonate well-known performers.

These contextual distinctions have obscured deeper thinking about whether the deepfakes across these and other contexts are (or should be) different from one another from a jurisprudential perspective. A more nuanced parsing of deepfakes is essential to better distinguish between the problems that are appropriate for legal redress versus those that are more appropriate for collective bargaining or market-based solutions, or that simply must be tolerated and in some instances even celebrated. The focus on the context in which deepfakes appear rather than on their other characteristics has also exacerbated the spread of overlapping and sometimes conflicting laws that cover a person's identity.[30] These contextually-targeted laws also may be less likely to survive constitutional challenges in part because their contextual targeting may make them underinclusive at addressing the problems at hand.[31]

I divide deepfakes (of humans) into four categories: *unauthorized*; *authorized*; *deceptively-authorized*; and *fictional*.

30. *See* Rothman, *supra* note 19, at 1278–88 (describing some of these overlapping laws before the recent explosion in AI-related legislation that has worsened the problem).

31. *See, e.g.*, Kohls v. Bonta, 797 F.Supp.3d 1177 (E.D. Cal. 2025) (striking down as unconstitutional recent California law regulating deepfakes in the election context in part because was underinclusive and viewpoint discriminatory); *cf.* 281 Care Committee v. Arneson, 766 F.3d 774 (8th Cir. 2014) (holding unconstitutional a Minnesota statute that made it a crime to knowingly or with reckless disregard for the truth make a false statement about a proposed ballot initiative in part because was underinclusive).

A. UNAUTHORIZED DEEPFAKES

Most of the expressed concerns over deepfakes have centered on the unauthorized use of a person's likeness, voice, or performance in ways that they never agreed to and that could deceive viewers or listeners into thinking that the person actually appeared or performed in the disseminated works. Recent calls for legislative action around deepfakes have stemmed from high-profile examples of such unauthorized uses, including the 2023 viral AI-generated song, "Heart on My Sleeve," which imitated the voices of successful recording artists Drake and The Weeknd.[32] The song became a hit and people thought it was an authentic new release from the famous artists.[33] Numerous other recording artists and actors have found themselves depicted in deepfakes. They are often shown falsely endorsing products, such as Tom Hanks being deceptively used in an ad for dental services, Taylor Swift "peddl[ing]" Le Creuset Cookware, or the recent fake Will Ferrell Doritos ad.[34]

The famous and the ordinary have been depicted by classmates, former partners, and strangers in pornographic contexts that they never appeared in using generative AI technology.[35] Politicians too have been victims of unauthorized and deceptive uses

32. *See* THE DAILY, *The Ballad of "Deepfake Drake"* (N.Y. Times Podcasts, Apr. 28, 2023), https://www.nytimes.com/2023/04/28/podcasts/the-daily/ai-deepfake-drake.html [https://web.archive.org/web/20260207024948/https://www.nytimes.com/2023/04/28/podcasts/the-daily/ai-deepfake-drake.html]; Chris Willman, *AI-Generated Fake "Drake"/"Weeknd" Collaboration, "Heart on My Sleeve," Delights Fans and Sets Off Industry Alarm Bells*, VARIETY (Apr. 17, 2023), https://variety.com/2023/music/news/fake-ai-generated-drake-weeknd-collaboration- heart-on-my-sleeve-1235585451/ [https://web.archive.org/web/20260207025005/https://variety.com/2023/music/news/fake-ai-generated-drake-weeknd-collaboration-heart-on-my-sleeve-1235585451/].

33. *See* Willman, *supra* note 32.

34. Michaela Zee, *Tom Hanks Warns Fans About "AI Version of Me" Promoting Dental Plan: "I Have Nothing to Do With It,"* VARIETY (Oct. 1, 2023), https://variety.com/2023/film/news/tom-hanks-ai-video-dental-plan-warns-fans-1235741781/ [https://web.archive.org/web/20260207025138/https://variety.com/2023/film/news/tom-hanks-ai-video-dental-plan-warns-fans-1235741781/]; Tiffany Hsu & Yiwen Lu, *No, That's Not Taylor Swift Peddling Le Creuset Cookware*, N.Y. TIMES (Jan. 9, 2024), https://www.nytimes.com/2024/01/09/technology/taylor-swift-le-creuset-ai-deepfake.html [https://web.archive.org/web/20260220181022/https://www.nytimes.com/2024/01/09/technology/taylor-swift-le-creuset-ai-deepfake.html]; *see also* ASTRO DYNAMICS, *Will Ferrell Doritos Super Bowl 2025 Ad* (YouTube, Feb. 2, 2025), https://www.youtube.com/watch?v=CLCy3H1ABj0 [https://web.archive.org/web/20260207025118/https://www.youtube.com/watch?v=CLCy3H1ABj0] (AI-generated fake ad not authorized by Ferrell or Doritos).

35. *See, e.g.*, Ashley Belanger, *NJ Teen Wins Fight to Put Nudify App Users in Prison, Impose Fines up to $30k*, ARS TECHINICA (Apr. 4, 2025), https://arstechnica.com/tech-policy/2025/04/adults-told-her-to-move-on-instead-teen-won-fight-to-criminalize-deepfakes/ [https://web.archive.org/web/20260207025623/https://arstechnica.com/tech-policy/2025/04/adults-told-her-to-move-on-instead-teen-won-fight-to-criminalize-deepfakes/] (describing such an incident involving teens in New Jersey, as well as legislation passed to address it within the state); Imran Rahman-Jones, *Taylor Swift Deepfakes Spark Calls in Congress for New Legislation*, BBC (Jan. 27, 2024), https://www.bbc.com/news/technology-68110476 [https://web.archive.org/web/20260207025704/https://www.bbc.com/news/technology-68110476]; Rachel DeSantis, *Kristen Bell Recalls Shock of Learning her Face Was Used in Pornographic Deepfake: "It's Not OK,"*

of their identities, including Presidents Joe Biden and Barack Obama, Senator Amy Klobuchar, and U.K. Prime Minister Rishi Sunak.[36] Deepfakes, particularly voice clones, have been used to deceive family members into thinking their relative is in danger, leading them to pay out large sums to criminals.[37] This technology is getting better every day, and Open AI's recent release of Sora 2 has generated significant concerns with its swift ability to generate authentic-seeming performances using the identities of real actors (and anyone else) based on ingesting existing performances.[38]

PEOPLE (June 10, 2020), https://people.com/human-interest/kristen-bell-shock-face-used-pornographic-deepfake/ [https://web.archive.org/web/20260207025757/https://people.com/human-interest/kristen-bell-shock-face-used-pornographic-deepfake/].

36. *See* Cristina Criddle, *Political Deepfakes Top List of Malicious AI Use, DeepMind Finds*, FIN. TIMES (June 25, 2024), https://www.ft.com/content/8d5bc867-c69d-44df-839f-d43c92785435 [https://web.archive.org/web/20260207025801/https://www.ft.com/content/8d5bc867-c69d-44df-839f-d43c92785435]; Joan Donovan & Britt Paris, *Beware the Cheapfakes*, SLATE (June 12, 2019), https://slate.com/technology/2019/06/drunk-pelosi-deepfakes-cheapfakes-artificial-intelligence-disinformation.html [https://web.archive.org/web/20260207025807/https://slate.com/technology/2019/06/drunk-pelosi-deepfakes-cheapfakes-artificial-intelligence-disinformation.html] (describing impact of low tech fakes, including "Drunk Pelosi," in which a video was slowed down to produce the effect of making it seem that Representative Pelosi was drunk when she was not); Victoria Elliott & Makena Kelly, *The Biden Deepfake Robocall Is Only the Beginning*, WIRED (Jan. 23, 2024), https://www.wired.com/story/biden-robocall-deepfake-danger/ [https://web.archive.org/web/20260207025953/https://www.wired.com/story/biden-robocall-deepfake-danger/] (describing a voice clone of President Biden that discouraged voting); Amy Klobuchar, *What I Didn't Say About Sydney Sweeney*, N.Y. TIMES (Aug. 20, 2025), https://www.nytimes.com/2025/08/20/opinion/amy-klobuchar-deepfakes.html [https://web.archive.org/web/20260207025913/https://www.nytimes.com/2025/08/20/opinion/amy-klobuchar-deepfakes.html]. This concern over the political dangers of deepfakes is not new to this generative AI moment. It was well illustrated by Jordan Peele's use of the technology to fake authentic videos of former President Barack Obama, intended to warn of the potential for inciting a war if world leaders are portrayed saying things they never said that could potentially launch wars. *See* Hallie Jackson, *Fake Obama Warning About "Deep Fakes" Goes Viral*, MS NOW (Apr. 19, 2018), https://www.ms.now/hallie-jackson/watch/fake-obama-warning-about-deep-fakes-goes-viral-1214598723984 [https://web.archive.org/web/20260207030047/https://www.ms.now/hallie-jackson/watch/fake-obama-warning-about-deep-fakes-goes-viral-1214598723984].

37. *See, e.g.*, Charles Bethea, *The Terrifying A.I. Scam That Uses Your Loved One's Voice*, NEW YORKER (Mar. 7, 2024), https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice [https://web.archive.org/web/20260301044605/https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice].

38. THE TOWN WITH MATTHEW BELLONI, *Sora 2, AI Actors, and How Hollywood Can Fight Back* (Puck, Oct. 2, 2025), https://puck.news/podcast_episode/sora-2-ai-actors-and-how-hollywood-can-fight-back/ [https://web.archive.org/web/20260207030127/https://puck.news/podcast_episode/sora-2-ai-actors-and-how-hollywood-can-fight-back/]. Since the time of the lecture, as predicted, many other models have sprung up, notably Seedance 2.0, which recently received significant attention for its use to generate a short of movie stars Tom Cruise and Brad Pitt fighting and talking about Jeffrey Epstein. *See, e.g.*, Jake Kanter, *Cruise vs Pitt Deepfake: TikTok Owner's New AI Video Model Appears to Be Regurgitating Hollywood Movies on Epic Scale*, DEADLINE (Feb. 12, 2026), https://deadline.com/2026/02/cruise-vs-pitt-seedance-viral-ai-hollywood-videos-1236717127/ [https://web.archive.org/web/20260315013551/https://deadline.com/2026/02/cruise-vs-pitt-seedance-viral-ai-hollywood-videos-1236717127/]; FILMY ATTACK, *AI Brad Pitt vs Tom Cruise Brawl Shocks Internet!* (YouTube, Feb. 12, 2026), https://www.youtube.com/watch?v=noz_aofEpcs [https://perma.cc/ZHY6-S2ZH].

These unauthorized deepfakes can cause all of the harms identified in Part II, including personality-based and market-based harms to the person depicted. Some deepfakes will make clear that they are fake through disclosures, absurd situations, or unrealistic depictions or other tells. But even in these contexts the public could be deceived into thinking the fakes are authorized or sponsored by the person depicted. Regardless of whether the public is deceived, the person depicted may be exposed to the same personal and financial harms. Those who are financially or otherwise connected to the person depicted may also suffer harms from such unauthorized deepfakes without regard to whether they deceive the public.

It is important to note, however, that not all unauthorized deepfakes should be barred. This is particularly so when the public is not deceived as to their authenticity and the uses further significant speech values such as telling creative stories that reference historical events or that provide political commentary. Consideration of possible First Amendment and other speech-related defenses to legal claims arising out of uses of deepfakes is beyond the scope of this Lecture, but is important to flag.[39] It is also worth highlighting that such speech protections will be at their nadir if the deepfakes are likely to deceive the public into thinking they are authentic because rather than serving the objectives of the First Amendment in such instances, the deepfakes undermine public discourse and the search for truth by destabilizing the public's perception of actual events. First Amendment protections are also likely to be limited when the uses could substitute for the work of the person depicted, particularly in the context of performances.[40]

B. AUTHORIZED DEEPFAKES

Despite their dominance in the public narrative, not all deepfakes are unauthorized. In some instances, the people depicted have authorized the use of their voices, likenesses, or performances. These authorized deepfakes therefore do not pose injuries to the person depicted but they may still pose harms to the public if they are deceptive. When they do not deceive the public, these authorized deepfakes do not cause cognizable harms and should be allowed.

Authorized deepfakes are becoming increasingly common. The company Metaphysic, for example, creates digital replicas of real people with the permission and coordination of the underlying person. Metaphysic created a replica of the rap star

39. For an in-depth consideration of the First Amendment analysis in the context of right of publicity claims, *see* Post & Rothman, *supra* note 18 *passim*; *see also* ROTHMAN, *supra* note 18, at 138–59.

40. *See* Post & Rothman, *supra* note 18, at 102–05, 146–48; Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 575–76 (1977); *In re* NCAA Student-Athlete Name & Likeness Licensing Litig., 724 F.3d 1268 (9th Cir. 2013); Hart v. Elec. Arts, Inc., 717 F.3d 141 (3d Cir. 2013); *see also* Oral Argument at 9:26, *In re NCAA*, 724 F.3d 1268 (No. 10-15387), https://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000006196 [https://web.archive.org/web/20260207030144/https://www.ca9.uscourts.gov/media/video/?20120713/10-15387/] (Judge Bybee expressing concern that if avatars of athletes were allowed in a video game then a movie studio might be able to reanimate Tom Cruise in a new *Mission Impossible* movie without hiring him to perform).

Eminem for use in his music video for his song *Houdini*.[41] The video shows Eminem dancing with a younger, digital-replica version of himself.[42] Metaphysic also worked with film director Robert Zemeckis to create de-aged versions of the actors Tom Hanks and Robin Wright for the 2024 movie *Here*.[43] YouTube has been working on voice clone technology that allows users to generate new songs that are voiced by famous singers. The company has been testing this technology as part of its Dream Track tool and has obtained permission from Charlie Puth and at least eight other artists including John Legend, Sia, and Charlie XCX to use their voices in these new AI-generated songs. The tracks sound as if these artists created new performances even though the sound files are entirely digitally generated.[44] Outside of entertainment, authorized uses are also growing. Speechify is a text-to-speech reader initially developed to help those with dyslexia and other learning differences to access written works more easily. The company has partnerships with a number of celebrities, including Snoop Dogg and Gwyneth Paltrow, and uses voice clones of them to make it seem as if these well-known performers are reading texts aloud to the listeners.[45]

Each of these uses is authorized and each of these examples have been used in ways that are either disclosed to the audience that receives them or are used in ways that are unlikely to deceive those who see or hear them. This need not be the case, however. Authorized deepfakes could deceive their audience. When they do, the law should address them because these fakes could cause the same set of harms to the public as unauthorized uses. On the other hand, we should leave room for creative and beneficial uses of nondeceptive deepfakes when authorized by the people depicted.

41. Damien Scott, *How Eminem Used AI to Bring Slim Shady Back to Life*, BILLBOARD (July 17, 2024), https://www.billboard.com/music/rb-hip-hop/eminem-slim-shady-houdini-video-making-of-1235732708/ [https://web.archive.org/web/20260217072438/https://www.billboard.com/music/rb-hip-hop/eminem-slim-shady-houdini-video-making-of-1235732708/].

42. EMINEMMUSIC, *Eminem—Houdini [Official Music Video]*, (YouTube, May 31, 2024), https://www.youtube.com/watch?v=22tVWwmTie8 [https://web.archive.org/web/20260301151713/https://www.youtube.com/watch?v=22tVWwmTie8].

43. Benj Edwards, *New Zemeckis Film Used AI to De-Age Tom Hanks and Robin Wright*, ARS TECHNICA (Nov. 24, 2024), https://arstechnica.com/ai/2024/11/new-zemeckis-film-used-ai-to-de-age-tom-hanks-and-robin-wright/ [https://web.archive.org/web/20260221220936/https://arstechnica.com/ai/2024/11/new-zemeckis-film-used-ai-to-de-age-tom-hanks-and-robin-wright/].

44. Eileen AJ Connelly, *YouTube Reveals "Dream Track," an Al Music Generator Using Nine Famous Singers' Sounds*, WRAP (Nov. 16. 2023), https://www.thewrap.com/youtube- dream-track-explained-ai-songs-charlie-puth-demi-lovato/ [https://web.archive.org/web/20260207030200/https://www.thewrap.com/youtube-%20dream-track-explained-ai-songs-charlie-puth-demi-lovato/]; YOUTUBE, *Introducing Dream Track—an experiment on YouTube Shorts—featuring Charlie Puth*, (YouTube, Nov. 14, 2023), https://www.youtube.com/watch?v=1gjuHUy0IMM [https://web.archive.org/web/20260207030307/https://www.youtube.com/watch?v=1gjuHUy0IMM].

45. SPEECHIFY, https://speechify.com/ [https://web.archive.org/web/2/https://speechify.com/] (last visited Feb. 20, 2026).

C. DECEPTIVELY-AUTHORIZED DEEPFAKES

A third category of deepfakes is often overlooked but essential to understand as a distinct category. Here a person may have agreed to appear in one work or recording but they did not agree to have their voice, likeness, or performance reused in a new context, such as a deepfake. Or, alternatively, the depicted person may not own or control the rights to their own name, likeness, or voice. In each of these scenarios, deepfakes might be categorized as "authorized" in a legal sense but in fact are "unauthorized" in the most important sense because the person whose voice or image is used in the deepfake did not knowingly approve of the specific use. I designate these deepfakes as *deceptively-authorized deepfakes*. These deceptively-authorized deepfakes cause the very same harms to the depicted person that form the basis for regulating deepfakes in the first place. These deceptively-authorized deepfakes also presumptively deceive the public into thinking the person depicted authorized them.

In prior work, I have questioned the legitimacy and constitutionality of allowing someone other than the person themselves—what I have dubbed the "identity-holder"—to own that person's name, likeness, or voice.[46] I have also warned about allowing broad licenses that would give long-term and extensive control over a person's identity to someone other than the identity-holder.[47] Yet, some new and longstanding state laws suggest such transfers and broad licenses may be possible, and several recently proposed bills in Congress to address deepfakes allow someone other than the identity-holder to own or control that person's digital replica.[48] Minors, student-athletes, aspiring actors, recording artists, and models may be particularly vulnerable to having others take control, or even ownership of their voices, likenesses, and performances.[49] But each of us is also at risk as we agree to online terms of service that we do not read

46. ROTHMAN, *supra* note 18, at 115–37; Jennifer E. Rothman, *The Inalienable Right of Publicity*, 101 GEO. L.J. 185, 191 (2012); *see also* Rothman, *supra* note 19, at 1309–17, 1325–31 (considering challenges to the transferability of personal marks in the context of trademark law).

47. *See* Rothman, *supra* note 46, at 234–36; Jennifer E. Rothman, *Reintroduced No FAKES Act Still Needs Revision*, REGUL. REV. (Aug. 18, 2025) (critiquing proposed licensing regime which does not adequately protect identity-holders), https://www.theregreview.org/2025/08/18/rothman-reintroduced-no-fakes-act-still-needs-revision/ [https://web.archive.org/web/20260207030338/https://www.theregreview.org/2025/08/18/rothman-reintroduced-no-fakes-act-still-needs-revision/].

48. *See, e.g.*, TENN. CODE ANN. § 47-25-1103 (stating that property rights to a person's "name, photograph, voice, or likeness" are all "freely assignable"); NO FAKES Act of 2025, *supra* note 6 (proposing ten-year licensing terms with insufficient limits); No AI FRAUD Act, H.R. 6943, 118th Cong. (2024) (authorizing wholesale transfer of a person's rights to their own voices and likenesses in context of digital replicas).

49. *See Artificial Intelligence and Intellectual Property: Part II—Identity in the Age of AI: Hearing Before the Subcomm. on Cts., Intell. Prop. & the Internet*, 118th Cong. 9–10 (2024) (Statement of Jennifer E. Rothman), available at https://rightofpublicityroadmap.com/wp-content/uploads/2024/02/Rothman_Statement_Subcommittee-on-IP_February-2_2024_Submitted.pdf [https://web.archive.org/web/20260207030456/https://rightofpublicityroadmap.com/wp-content/uploads/2024/02/Rothman_Statement_Subcommittee-on-IP_February-2_2024_Submitted.pdf].

and that claim to be able to use our images and recordings in new contexts, including deepfakes, without our permission.[50]

Deceptively-authorized deepfakes raise complicated questions about the intersection of a variety of legal regimes, including contract law, state publicity rights, and federal copyright law. One recent case, *Lehrman v. Lovo*, raises this issue.[51] The company Lovo reached out to two voiceover actors and paid them to record and then use their voices in the development of its text-to-speech software. The actors were told the uses would be for "research purposes only."[52] The company, however, went on to clone the actors' voices and use them more broadly without obtaining additional permission or paying them for the uses—even asserting to customers that the uses were authorized and the outputs were legitimately available for use by their customers.[53] This case could be understood as an unauthorized deepfake case, but the initial voice clones were created with authorization and to the extent such initial captures were protected by copyright, copyright could enable such uses.[54] We will increasingly see cases like this in which a person agreed to one use but not another.[55]

Even though the scale and nature of the problem is growing because a person's performance can so easily be replicated and in ways that are difficult to detect, this problem is longstanding.[56] If a person gives permission to be captured in a copyrighted work, then this work can be reused, including in derivative works, under federal law. This circumstance has led to a number of lawsuits, raising the question of whether state right of publicity laws—that prohibit unauthorized uses of a person's name, voice, or likeness—are preempted by copyright law in such instances. Consider the *Laws v. Sony Music* case, in which a singer's recording was reused in a new recording without her additional permission. The Ninth Circuit Court of Appeals concluded that copyright

50. *See, e.g.*, *Terms of Service*, X, https://x.com/en/tos [https://perma.cc/7ZWZ-J5YE] (last visited Feb. 20, 2026) (providing license to X to use, adapt, modify, and transform any media uploaded to platform); *Terms of Use*, INSTAGRAM, https://help.instagram.com/termsofuse [https://perma.cc/MM8Y-9REP?type=image] (last visited Mar. 1, 2026) (providing license to modify media uploaded to platform, in addition to the right to "prepare derivative works"); *see also Artificial Intelligence and Intellectual Property*, *supra* note 49, at 9–10.

51. Lehrman v. Lovo, Inc., 790 F. Supp. 3d 348 (S.D.N.Y. 2025).

52. *Id.* at 356.

53. *Id.*

54. *Id.* at 381–82, 388 (allowing right of publicity/privacy claims to proceed beyond the motion to dismiss stage under N.Y. Civil Rights Law §§ 50–51).

55. *Cf.* Complaint, Vacker v. Eleven Labs, No. 1:24-cv-00987-UNA (D. Del., Aug 9., 2024) (alleging that AI voice cloning company violated publicity rights of voice-over actors). The case recently settled without any court determination. *See* Joint Stipulation of Voluntary Dismissal with Prejudice, Vacker v. Eleven Labs, No. 1:24-cv-00987-UNA (D. Del., Nov. 5, 2025).

56. *See, e.g.*, Laws v. Sony Music Ent., Inc., 448 F.3d 1134 (9th Cir. 2006); Toney v. L'Oreal USA, Inc., 406 F.3d 905 (7th Cir. 2005); Ahn v. Midway Mfg. Co, 965 F. Supp. 1134 (N.D. Ill. 1997); Eriq Gardner, *"Back to the Future II" from a Legal Perspective: Unintentionally Visionary*, HOLLYWOOD REP. (Oct. 21, 2015) https://www.hollywoodreporter.com/business/business-news/back-future-ii-a-legal-833705/ [https://web.archive.org/web/20260207030629/https://www.hollywoodreporter.com/business/business-news/back-future-ii-a-legal-833705/] (describing film's use of old and new footage to make it seem like same actor appeared in second *Back to the Future* movie when he did not); *see also* ROTHMAN, *supra* note 18, at 167–77 (giving examples of these conflicts).

law allowed such licensing by the copyright holder without requiring additional permission of the singer and preempted her state publicity claim.[57]

Other cases have also allowed the reuse of actors and singers' performances on the basis of copyright law. For example, in *Ahn v. Midway Manufacturing*, a case from the 1990s, a district court held that martial artists and actors' performances used in one video game edition could be used in another version of the video game without requiring additional consent by the performers.[58] One of the few cases to swing the other direction involved the band No Doubt's lawsuit against Activision, which allowed a right of publicity claim to proceed in spite of the authorization to have digital versions of the band appear and sing in a video game because the uses exceeded the boundaries of the relevant contracts.[59]

Copyright law could make reuses of copyrighted material in deepfakes "authorized" even though they would be created without the specific approval of the person depicted and in ways that might deceive the public. This explains why the major actors' union, SAG-AFTRA, is worried about using copyright law in this way and about the scope of prior employment contracts, which were drafted and signed before the world of digital replicas in which we are currently living.[60] It is an open question whether digital replicas are copyrightable. If they are, this may further risk a person agreeing to the capture of their digital replica in one context and then losing control over what is done with this replica; a copyright holder is authorized to reuse the copyrighted material in future works and such reuses are often (though not always) allowed on the basis of copyright law preempting state right of publicity claims.[61]

Federal laws addressing deepfakes could combat the preemptive effect of copyright law in such instances, but if the laws are drafted in ways that also empower third parties to deceptively authorize deepfakes this will worsen the problem of deceptively-authorized deepfakes. Recent proposed legislation at the federal level and some bills passed at the state level explicitly create a digital replica right—originating in the underlying person—but allow someone else to either own these rights or have long-term and largely unrestricted licenses to use them.[62] Some bills explicitly allow "authorized representatives" to approve uses of a person's digital replica without

57. *Laws*, 448 F.3d at 1145–46. The court suggested that the plaintiff Laws might have a contract claim against the original record label, but since the case involved a licensee that issue was not before the court.

58. *Ahn*, 965 F. Supp. at 1140.

59. *See* No Doubt v. Activision Publ'g, 702 F. Supp. 2d 1139 (C.D. Cal. 2010).

60. Press Release, SAG-AFTRA, Gov. Newsom Signs Union-Championed A.I. Bills at SAG-AFTRA Plaza (Sep. 17, 2024), https://www.sagaftra.org/gov-newsom-signs-union-championed-ai-bills-sag-aftra-plaza.

61. *See* Jennifer E. Rothman, Donald C. Brace Lecture, *Copyrighting People*, 72 J. COPYRIGHT SOC'Y 1, 7–9, 17, 26–33 (2025).

62. NO FAKES Act of 2025, *supra* note 6; No AI FRAUD Act of 2024, *supra* note 48; TENN. CODE ANN. § 47-25-1101 *et seq.* (2024) (replacing in its entirety prior publicity statute with the ELVIS Act, Tenn. H.B. 2091, passed in 2024, largely to address digital replicas); CAL. LAB. CODE § 927 (West 2024) (added in 2024 by A.B. 2602, 2023–2024 Leg., Reg. Sess. (Cal. 2024)) (allowing the "creation and use of a digital replica of a person's voice or likeness in place of work the individual would otherwise have performed" without requiring approval of specific uses of replica by person depicted).

requiring any consultation with the person as to how the replica of them is used.[63] Even if legislation limits the duration of such licenses, the digital replicas will likely be able to be reused after their expiration. If the digital replicas are copyrightable or contained within copyrighted works, copyright law expressly allows such continued uses and notably also allows new derivative works to be created from them.[64] There is also a danger that parents could authorize deepfakes of their children for their own financial profits. These too are technically "authorized" in a legal sense, but also unauthorized in the sense that the minors themselves may not have had any say in how they are depicted.[65]

The question of deceptively-authorized deepfakes also arises with somewhat different implications in the context of the dead. Obviously, we cannot authorize uses from the grave, so in one sense no uses of deepfakes of dead people are authorized. However, if we create postmortem rights in the identities of the dead as some state laws do, and as several federal bills have proposed, then uses of the dead could be authorized by their estates or by corporations that own or control their identities.

In short, deceptively-authorized deepfakes cause the same potential harms as unauthorized deepfakes both to the underlying person (if alive) and to the public at large if the fakes are deceptive as to their authenticity or sponsorship. Accordingly, legislation targeting deepfakes needs to address such deceptively-authorized deepfakes, rather than incentivize them. In such instances, we might want to consider who should have the authority to agree to such uses and for how long, as well as whether we should follow the decedents' wishes, if known.[66]

D. FICTIONAL DEEPFAKES

The final category of deepfakes does not involve fakes of real people—instead, they are entirely AI-generated. I dub these *fictional deepfakes*. Of course, all deepfakes are fictional in the broader sense of depicting something that is not real, even though the images or sounds appear authentic. My point here by calling them "fictional" is to emphasize that those depicted are themselves fictional constructs rather than depictions of real, identifiable natural persons. The "people" who are depicted in these

63. NO FAKES Act of 2025, *supra* note 6; *see also* TENN. CODE ANN. §§ 47-25-1103, 47-25-1106(f) (allowing rights to a person's voice or likeness to be transferred to others without limitation and allowing those holding contracts with "recording artist[s]" or that hold licenses for "sound recordings" to enforce rights in another person's voice and likeness); CAL. LAB. CODE § 927 (West 2024) (allowing union to authorize uses of members' digital replicas without consultation with specific person depicted).

64. *See, e.g.*, Laws v. Sony Music Ent., Inc., 448 F.3d 1134 (9th Cir. 2006); *see also supra* notes 56-60 and accompanying text.

65. The NO FAKES Act of 2025, *supra* note 6, is one of the few proposed bills to consider additional protections for minors, notably including court review of such licenses. Even with this added layer of protection, the bill does not address the reuse of digital replicas of minors created during the licensing term after the expiration of the licensing periods, and it allows authorized representatives (perhaps authorized by a minor's parent or guardian) to continue to authorize uses even after a minor has turned eighteen.

66. *See* Allen & Rothman, *supra* note 19, at 333-49 (considering appropriate limits on who can bring postmortem claims and how long such rights should persist, as well as supporting the decedent's preferences in some instances).

deepfakes do *not* exist. Consider the recent coverage of the AI-generated actor Tilly Norwood, who is shown speaking and emoting in short clips in realistic ways,[67] or AI-generated fashion models, or AI-generated songs and music filling Spotify's playlists.[68]

The harms that flow from deepfakes that depict entirely synthetic creations are quite different from deepfakes that depict real and identifiable individuals. Fictional deepfakes might deceive the public into thinking they depict real people, but there is not an underlying person who could suffer harms from such a use. Such fictional deepfakes, however, should still be regulated when they are likely to deceive the public into thinking they depict authentic people. In such instances, the same harms to the public can flow from these deceptive fakes of fictional constructs as do from depictions of real people. If, however, these fictional deepfakes are disclosed or obvious, then they should generally be allowed.

Even though deceptive fictional deepfakes should be regulated, the government should allow room for technological disruption and should not be in the business of determining our preferred diet of music and entertainment. Just as actors must tolerate a reduction in on-screen acting jobs because of the success of reality television, animated shows, and sports broadcasts, actors (and recording artists and models) will

---

67. Gene Maddaus, *Tilly Norwood Creator on Hollywood Backlash Creating Jobs and Full AI Movies: "I Don't Think" People Will "Know the Difference,"* VARIETY (Nov. 11, 2025), https://variety.com/2025/film/news/tilly-norwood-creator-eline-van-der-velden-ai-actress-1236574125/ [https://web.archive.org/web/20251229142308/https://variety.com/2025/film/news/tilly-norwood-creator-eline-van-der-velden-ai-actress-1236574125/]; Leo Barraclough, *AI Actress Tilly Norwood Debuts at Zurich Summit as Industry Grapples with Emerging Tech: We Want Her "to be the Next Scarlett Johansson,"* VARIETY (Sep. 28, 2025), https://variety.com/2025/film/global/ai-actress-tilly-norwood-talent-agents-zurich-summit-1236533454/ [https://web.archive.org/web/20260205222845/https://variety.com/2025/film/global/ai-actress-tilly-norwood-talent-agents-zurich-summit-1236533454/].

68. *See* Ali Rogan, *AI-Generated Models Shake Up the Fashion Industry and Raise Concerns* (Aug. 16, 2025), PBS NEWS, https://www.pbs.org/newshour/show/ai-generated-models-shake-up-the-fashion-industry-and-raise-concerns [https://web.archive.org/web/20260205223934/https://www.pbs.org/newshour/show/ai-generated-models-shake-up-the-fashion-industry-and-raise-concerns]; SERAPHINNE VALORA, https://www.seraphinnevallora.com/ [https://web.archive.org/web/20260205224009/https://www.seraphinnevallora.com/] (describing AI-focused marketing agency); Sarah Perez, *Spotify to Label AI Music, Filter Spam and More in AI Policy Change*, TECHCRUNCH (Sept. 25, 2025), https://techcrunch.com/2025/09/25/spotify-updates-ai-policy-to-label-tracks-cut-down-on-spam/ [https://web.archive.org/web/2/https://techcrunch.com/2025/09/25/spotify-updates-ai-policy-to-label-tracks-cut-down-on-spam/]; Brian Hiatt, *AI "Band" The Velvet Sundown Confirm They're AI—and a "Provocation,"* ROLLING STONE (July 5, 2025), https://www.rollingstone.com/music/music-features/ai-band-the-velvet-sundown-confirm-ai-1235379354/ [https://web.archive.org/web/20260205224253/https://www.rollingstone.com/music/music-features/ai-band-the-velvet-sundown-confirm-ai-1235379354/]; *see also* Ethan Millman, *Spotify to Develop AI Music Products in Partnership with Major Record Labels*, HOLLYWOOD REP. (Oct. 16, 2025), https://www.hollywoodreporter.com/music/music-industry-news/spotify-ai-music-partnership-with-record-labels-1236402698/ [https://web.archive.org/web/20260205224338/https://www.hollywoodreporter.com/music/music-industry-news/spotify-ai-music-partnership-with-record-labels-1236402698/] (describing partnership with Universal Music Group, Sony Music Group, and Warner Music group to develop AI music products).

need to tolerate some computer-generated performances.[69] Unions may want to use collective bargaining agreements to require or maximize uses of real actors, but the law should not mandate this.

With that said, there may be questions as to whether the training of some of the AI-generated characters violates the rights of the real people whose performances or identities were used to train these AI "actors."[70] Additionally, if AI outputs too closely resemble a real person, there could also be potential liability under some of the claims that I consider next in Part IV.

* * *

Along with the parade of horribles that flows from deepfake and generative AI technology there is also much to celebrate about this technology. Deepfake technology can improve (and reduce the costs) of visual effects and enhance storytelling and art. The same technology can help those who have lost or are losing the ability to speak to communicate or allow people to use their own voice to speak in foreign languages.[71] The technology can create interactive replicas of deceased loved ones—something that some of us may regard as creepy but others as profound and comforting.[72] The technology can train the police, members of the military, and others using realistic virtual experiences.[73] It can help those with dyslexia and ADHD engage with printed

69. Animated works usually hire voice actors to voice the characters. These jobs are also at risk with AI-generated voice technology.

70. There are allegations that Tilly Norwood was trained on multiple performances of real people. *See* Conor Murray, *SAG-AFTRA Condemns AI "Actress" Tilly Norwood—Joins Critics Emily Blunt, Whoopi Goldberg and More*, FORBES (Sept. 30, 2025), https://www.forbes.com/sites/conormurray/2025/09/30/sag-aftra-condemns-ai-actress-tilly-norwood-joins-critics-emily-blunt-whoopi-goldberg-and-more/ [https://web.archive.org/web/20251202192449/https://www.forbes.com/sites/conormurray/2025/09/30/sag-aftra-condemns-ai-actress-tilly-norwood-joins-critics-emily-blunt-whoopi-goldberg-and-more/].

71. *See* April Dembosky, *People Who Have Lost Their Voices Are Using AI Technology to Regain Them*, NPR: ALL THINGS CONSIDERED (July 22, 2025), https://www.npr.org/2025/07/22/nx-s1-5449081/people-who-have-lost-their-voices-are-using-ai-technology-to-regain-them [https://web.archive.org/web/20260205224513/https://www.npr.org/2025/07/22/nx-s1-5449081/people-who-have-lost-their-voices-are-using-ai-technology-to-regain-them]; ELEVENLABS, https://elevenlabs.io/ [https://web.archive.org/web/20260205224541/https://elevenlabs.io/] (last visited Feb. 20, 2026) (providing translation into more than thirty languages using voice clones).

72. *See* Tharin Pillay, *"The Dead Have Never Been This Talkative": The Rise of AI Resurrection*, TIME (June 27, 2025), https://time.com/7298290/ai-death-grief-memory/ [https://web.archive.org/web/20260205224621/https://time.com/7298290/ai-death-grief-memory/]; *see also* Jake Kanter, *Michael Caine Partners with AI Company ElevenLabs to Clone His Voice*, DEADLINE (Nov. 11, 2025), https://deadline.com/2025/11/michael-caine-elevenlabs-voice-clone-1236613791/ [https://web.archive.org/web/20260205224900/https://deadline.com/2025/11/michael-caine-elevenlabs-voice-clone-1236613791/] (describing ElevenLabs having voice clone rights or licenses over a host of dead people, including Rock Hudson, John Wayne, Judy Garland, Maya Angelou, Amelia Earhart, and Mark Twain).

73. *See Rethinking Response Part Three: VR Training for Public Safety*, POLICING PROJECT, https://www.policingproject.org/rethinking-response-articles/2025/5/8/part-two-body-worn-camera-analytics-e3zg9-zlhxw [https://web.archive.org/web/20260205224812/https://www.policingproject.org/rethinking-response-

material that would otherwise be difficult to access by having familiar voices read the texts out loud.[74]

We cannot and should not legislate our way out of all market and labor disruptions caused by new technology, but we can require that deepfakes be authorized by the person depicted and that they not deceive the public into thinking the fakes are authentic. With this taxonomy and these benchmarks in hand we can now consider the legal landscape in the United States.

IV. THE LEGAL LANDSCAPE IN THE UNITED STATES

The recent vintage of the term deepfakes (and similar terms, like digital replicas) may explain why calls for new laws to address them have overlooked the many longstanding laws that already address unauthorized uses of a person's identity and that likely apply to unauthorized deepfakes. The concerns expressed in the opening demonstration of today's symposium raised the question of whether Taylor Swift would have claims for an unauthorized deepfake of her. The answer is she would have many potential claims. This is a different question than whether a nonprofit creation of such a deepfake for educational and demonstrative purposes would nevertheless be allowable where abundant efforts were made to highlight that there was no affiliation, participation, or sponsorship by Swift. Such a use would likely either fall outside the scope of some claims or be protected by the First Amendment.

Let's consider as a starting point some of the many laws currently on the books that would give claims to those depicted in deepfakes, whether they are megastars or not. My focus will be primarily, though not exclusively, on claims that could be brought by the real, natural person depicted.

A. STATE LAWS

1. The Right of Publicity/Appropriation Tort

At the heart of the legal regime in the United States that protects identity rights is the right of publicity—a state law, which is also sometimes part of or synonymous with

articles/2025/5/8/part-two-body-worn-camera-analytics-e3zg9-zlhxw] (last visited Feb. 21, 2026); Daniel Coates, *"Realism of the Scenario": Lowell Police Rolls Out Immersive, Virtual Reality Training Machine*, BOS. 25 NEWS (Nov. 6, 2025), https://www.boston25news.com/news/local/realism-scenario-lowell-police-rolls-out-immersive-virtual-reality-training-machine/ZDCVFUAADZFKXNCUE4I56SWZ2A/ [https://web.archive.org/web/20260205225109/https://www.boston25news.com/news/local/realism-scenario-lowell-police-rolls-out-immersive-virtual-reality-training-machine/ZDCVFUAADZFKXNCUE4I56SWZ2A/].

74. *See* John Boitnott, *This Immigrant Founder Taught Himself English—Then Made an App that Helps Others with His Disability (and Speed Readers)*, INC. (Aug. 29, 2017), https://www.inc.com/john-boitnott/how-one-founder-turned-his-dyslexia-into-an-app-th.html [https://web.archive.org/web/20251204113902/https://www.inc.com/john-boitnott/how-one-founder-turned-his-dyslexia-into-an-app-th.html].

privacy laws focused on the misappropriation of a person's identity.[75] In broad strokes, right of publicity laws and the appropriation tort provide civil liability (and sometimes criminal penalties) for unauthorized uses of a person's identity.[76] Liability can arise for uses of a person's name, likeness, voice, or performance, as well as for uses of other indicia of a person's identity.[77] These laws date to the early 1900s and have long protected both commercial and personal interests, and both the famous and the ordinary.[78] Even though these laws are more than one hundred years old, they apply without regard to the technology employed and therefore provide claims in the context of the deepfakes of today.

Almost every state provides either a common law or statutory state law claim that protects against unauthorized uses of a person's name, likeness, voice, or other indicia of identity, and no state has rejected such a right for the living.[79] The boundaries differ in some respects but many states track broad protections provided by the common law appropriation tort (even when adopted by statute). I will provide a few illustrative examples, focusing on the three states that are currently the most active in right of publicity litigation or legislation. First, California—California actually has three or four general right of publicity laws depending on how you count them. The state's common law right of publicity, which should be understood as synonymous with its privacy-based appropriation tort, provides that: "To establish a common law claim a plaintiff must prove: (1) the defendant used the plaintiff's identity; (2) the appropriation was for defendant's advantage, commercially or otherwise; (3) lack of consent; and (4) resulting injury."[80] This law covers unauthorized uses of a person's image or voice in deepfakes

75. *See, e.g.*, Zacchini v. Scripps-Howard Broad. Co., 351 N.E.2d 454, 458–60 (Ohio 1976) (explaining that Ohio's right of privacy encompasses a claim for the "appropriation of a plaintiff's name and likeness" and that "this aspect of privacy" is termed "the right of publicity"), *rev'd on other grounds*, 433 U.S. at 565–66 (understanding plaintiff's state right of privacy claim as one for the violation of the right of publicity); Prima v. Darden Rests., Inc., 78 F. Supp. 2d 337, 346 (D.N.J. 2000) ("Louisiana law . . . does not expressly provide for a right of publicity. Rather, courts in Louisiana have interpreted Louisiana's right of privacy to protect a person's name or likeness from commercial exploitation.") (citing Prudhomme v. Procter & Gamble Co., 800 F. Supp. 390, 396 (E.D. La. 1992)); Brinkley v. Casablancas, 438 N.Y.S.2d. 1004, 1012 (N.Y. App. Div. 1981) (concluding that New York's privacy statute is the state's "right of publicity"); *see also* RESTATEMENT (SECOND) OF TORTS § 652C (1977) (treating the privacy-based appropriation tort and the right of publicity as identical); ROTHMAN, *supra* note 18, at 11–86; Post & Rothman, *supra* note 18, at 93–95.

76. *See* RESTATEMENT (SECOND) OF TORTS § 652C (1977); Eastwood v. Superior Court, 149 Cal. App.3d 409, 416–17 (1983); N.Y. CIV. RIGHTS LAW §§ 50–51; *see also* ROTHMAN, *supra* note 18; ROTHMAN'S ROADMAP TO THE RIGHT OF PUBLICITY, https://rightofpublicityroadmap.com/ https://web.archive.org/web/20260226131359/https://rightofpublicityroadmap.com/ (last visited Mar. 7, 2026) [hereinafter "ROTHMAN'S ROADMAP"].

77. *See, e.g.*, *Zacchini*, 433 U.S. 562; Jordan v. Jewel Food Stores, Inc., 743 F.3d 509 (7th Cir. 2014); Abdul-Jabbar v. General Motors Corp., 85 F.3d 407 (9th Cir. 1996); Waits v. Frito-Lay, Inc., 978 F.2d 1093 (9th Cir. 1992); White v. Samsung Elecs. Am., 971 F.2d 1395 (9th Cir. 1992); Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988); Motschenbacher v. R.J. Reynolds Tobacco Co., 498 F.2d 821 (9th Cir. 1974); *see also* ROTHMAN, *supra* note 18, 88–96 (describing history and sweep of right of publicity laws).

78. *See* ROTHMAN, *supra* note 18, at 27–44.

79. *See* ROTHMAN'S ROADMAP, *supra* note 76. States, such as New York, that initially rejected such a claim under their common law have subsequently adopted similar provisions by statute.

80. *Eastwood*, 149 Cal. App. 3d at 416–17.

and does so regardless of whether the person depicted has a commercially valuable identity and regardless of whether the use was a commercial one.

California's statutory right of privacy/publicity for the living, located in Civil Code § 3344, also covers deepfakes though with a narrower scope—limited to uses "on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services."[81] This law was passed to extend statutory damages and attorney's fees to people who were not celebrities to make such claims viable for ordinary people.[82] California's right of publicity for the dead was revised in 2025 to explicitly address digital replicas. The amendments to the statute remove the statutory exemption for uses in "audiovisual work[s]" in the context of digital replicas that depict "deceased personalit[ies]."[83] California's postmortem statute does not apply to everyone—something that I have criticized elsewhere—but only applies to well-known individuals who died with "commercial value" at the time of their death.[84]

New York's statutory privacy and publicity laws also cover deepfakes but might not cover noncommercial deepfakes because it is limited to claims that arise out of uses for advertising or trade purposes.[85] *Lehrman v. Lovo* is one of the first cases to hold that New York's statutory privacy/publicity law bars unauthorized voice clones.[86] New York's postmortem publicity right, which was added in 2020, explicitly covers deepfakes or digital replicas of dead people. Notably, the scope of the postmortem provision is very narrow, only applying to "deceased performers."[87]

Tennessee's 2024 overhaul of its right of publicity laws was expressly done to address concerns over deepfakes.[88] It added numerous provisions, including adding "voice" to its statutory bar on unauthorized uses of a person's identity, which now explicitly covers the unauthorized use of a person's "name, photograph, voice, or

81. CAL. CIV. CODE § 3344 (West 2024).

82. California's statutory right of publicity for the living, which is now frequently used to protect the commercial value of identity, was originally passed under the moniker of "privacy" and created to provide ordinary citizens whose identity lacked commercial value the opportunity to obtain statutory damages. Act of Nov. 22, 1971, ch. 1595, 1971 Cal. Stat. 3426 (*codified at* CAL. CIV. CODE § 3344 (West 2024)); ROTHMAN, *supra* note 18, at 208 n.40; Letter from John Vasconcellos, Member, Cal. State Assembly, to Ronald Reagan, Governor of Cal. (Nov. 10, 1971) (on file with the Cal. State Archives, Governor's Chaptered Bill File).

83. CAL. CIV. CODE § 3344.1 (West 2025). This postmortem statute was originally passed in 1984 (as CAL. CIV. CODE § 990) and long had exemptions for uses in various expressive and artistic contexts, notably including audiovisual works and accordingly there were concerns that digital replicas of the dead might be exempted from liability—something that was not the case with the right for the living which does not have similar exemptions either at common law or under the statute.

84. CAL. CIV. CODE § 3344.1; Allen & Rothman, *supra* note 19, at 335–36.

85. N.Y. CIV. RIGHTS LAW §§ 50–51.

86. Lehrman v. Lovo, Inc., 790 F. Supp. 3d 348 (S.D.N.Y. 2025) (allowing right of publicity/privacy claims to proceed beyond the motion to dismiss stage under N.Y. CIV. RIGHTS LAW §§ 50–51).

87. N.Y. CIV. RIGHTS LAW § 50-f. Deceased performers are narrowly defined as "a deceased natural person domiciled in [the State of New York] at the time of death who, for gain or livelihood, was regularly engaged in acting, singing, dancing, or playing a musical instrument." *Id.* § 50-f(1)(a).

88. TENN. CODE ANN. §§ 47-25-1101–1108 (2024) (replacing in its entirety the prior publicity statute with the ELVIS Act, passed in 2024).

likeness."[89] The law protects all people regardless of whether they commercialize their identities. The statute creates liability when unauthorized uses of a person's name, voice, or likeness are "for purposes of advertising products, merchandise, goods, or services, or for purposes of fundraising" or a "person publishes, performs, distributes, transmits, or otherwise makes available to the public an individual's voice or likeness, with knowledge that use of the voice or likeness was not authorized."[90] The statute also bars the distribution or making available of "an algorithm, software, tool, or other technology, service, or device, the primary purpose or function of [which] is the production of a particular, identifiable individual's photograph, voice, or likeness, with knowledge that distributing, transmitting, or otherwise making available the photograph, voice, or likeness was not authorized."[91] Thus, the law not only regulates the making of deepfakes but also the software that facilitates their creation and creates liability for knowing dissemination of deepfakes. It also makes clear that although an audiovisual work can represent a real person, it cannot do so in a way that is "intended to create, and does create, the false impression that the work is an authentic recording in which the individual participated."[92] Tennessee may also have a broader common law right of publicity.[93]

In short, most state right of publicity and privacy laws cover deepfakes,[94] but there are some reasons we might want more protection against deepfakes than these laws provide. First off, and importantly, most right of publicity laws allow deceptive uses so long as they are authorized by the publicity holder. Right of publicity laws therefore do not address authorized deepfakes that nevertheless deceive the public. Second, some of these right of publicity laws explicitly allow ownership or control by someone other than the person depicted.[95] Thus, they allow deceptively-authorized deepfakes—which, as I have observed, cause all of the same harms as unauthorized deepfakes. If such control by others is allowed, these laws could amplify rather than limit the deception of the public and also harm the individuals depicted.

89. TENN. CODE ANN. § 47-25-1105 (2024).

90. TENN. CODE ANN. §§ 47-25-1105(a)(1) & (2) (2024).

91. *Id.* § 47-25-1105(a)(3).

92. TENN. CODE ANN. § 47-25-1107(a)(3) (2024).

93. There is an open question of whether Tennessee also has a common law right of publicity/appropriation right or whether this right was "supplant[ed]" by the statute. *See* Marshall v. ESPN, Inc., 111 F. Supp. 3d 815, 824 (M.D. Tenn. 2015). No state court in Tennessee has ruled that the common law is preempted by the statute. *See, e.g.*, State *ex rel.* Elvis Presley Int'l Mem'l Found. v. Crowell, 733 S.W.2d 89 (Tenn. Ct. App. 1987) (indicating that the state recognizes both a common law and statutory right of publicity and privacy).

94. For some illustrative examples of publicity rights in other states that would cover deepfakes, *see, e.g.*, Ventura v. Titan Sports, Inc., 65 F.3d 725 (8th Cir. 1995) (recognizing common law publicity rights in Minnesota); Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998) (recognizing appropriation tort in Minnesota); Doe v. TCI Cablevision, 110 S.W.3d 363 (Mo. 2003) (recognizing both a common law right of publicity and an appropriation tort in Missouri, differentiated solely over whether use is for commercial advantage or any advantage); Hepp v. Facebook, 14 F.4th 204 (3d Cir. 2021) (recognizing both a statutory and common law right of publicity in Pennsylvania); Vogel v. W. T. Grant Co., 327 A.2d 133 (Pa. 1974) (recognizing common law appropriation tort in Pennsylvania).

95. *See, e.g.*, ALA. CODE § 6-5-771 (2024); CAL. LAB. CODE § 927 (2024); LA. REV. STAT. § 51-470.3; TENN. CODE ANN. §§ 47-25-1103, 47-25-1106 (2024).

Third, some state publicity laws limit claims to the context of commercial uses or for commercial advantage. This may make it difficult to make out a right of publicity case for deepfakes made by noncommercial entities and that are circulated for free in circumstances that are not meant to boost a person's commercial footprint. A number (albeit a minority) of states also limit who can bring claims to those with commercially valuable identities—primarily in the context of postmortem rights—which will make it hard for everyone to make out a publicity/privacy claim. Even in the vast majority of jurisdictions that allow ordinary people to bring publicity/appropriation claims, damages may be hard to prove and not all states provide statutory damages or fee-shifting provisions which would make such claims viable.[96]

Additionally, as discussed, copyright law may preempt state publicity claims if they arise out of deepfakes created by an authorized owner or licensee of copyrighted works used to create the fakes. There is also a circuit split on whether a federal law, the Communications Decency Act Section 230, may limit platform liability for right of publicity claims arising out of uses by third parties.[97] If platforms are immunized from such claims, they will have less of an incentive to remove unauthorized deepfakes, and plaintiffs will not be able to recover damages from the platforms.

Finally, the simple fact that we have fifty different state laws to navigate poses some challenges given the likely dissemination of works across the country and some variability across the states in what rights are extended.[98] Although most states recognize some form of the appropriation tort which is largely the same across jurisdictions, there is great variability in the statutory rights, especially with regard to the treatment of the dead.

---

96. Some states realizing this problem have added statutory damages and fee-shifting provisions to ensure that ordinary people are adequately protected and that there is a sufficient incentive not to use a person's identity without regard to their commercial value. California, for example, has long had statutory damages in its statutory publicity/privacy law, as well as a fee-shifting provision. CAL. CIV. CODE § 3344 (2025); *see also supra* note 82. California also recently passed a law increasing statutory damages to $250,000 for the "malicious" circulation of unauthorized intimate images, including deepfakes. *See* A.B. 621, 2025 Gen. Assemb., Reg. Sess. (Ca. 2025) (signed by governor Oct. 13, 2025); *see also, e.g.*, ALA. CODE § 6-5-774 (2024) (providing $5,000 statutory damages).

97. *Compare* Hepp v. Facebook, 14 F.4th 204 (3d Cir. 2021) (holding that § 230 does not bar state right of publicity claim from proceeding against Facebook) *with* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007) (holding that right of publicity claim could not proceed because of § 230 immunity); *see also* Jennifer E. Rothman, *Third Circuit Holds that Newscaster's Right of Publicity Claim Can Proceed Against Facebook*, ROTHMAN'S ROADMAP (Sep. 28, 2021), https://rightofpublicityroadmap.com/news_commentary/third-circuit-holds-that-newscasters-right-of-publicity-claim-can-proceed-against-facebook/ [https://web.archive.org/web/20260208092309/https://rightofpublicityroadmap.com/news_commentary/third-circuit-holds-that-newscasters-right-of-publicity-claim-can-proceed-against-facebook/]. Some states have tried to address this issue by expressly stating in statutes that the statutory publicity right (or related law) is a form of intellectual property for purposes of § 230. State statutes cannot, however, determine what is meant by a federal law. Nevertheless, if the federal law includes state intellectual property laws, then state designations may affect whether the § 230 exemption applies.

98. I note that to address some of this variability, I have been charged as the Reporter of the Uniform Law Commission's Study of Name, Image, and Likeness Rights to consider the possibility of drafting a uniform law to create greater uniformity across state laws.

2. Other State Laws Targeting Identity Rights

Right of publicity laws are not the only state laws that apply to deepfakes. Many other state statutes specifically target identity rights and cover deepfakes. These include intimate image laws,[99] biometric privacy laws,[100] impersonation laws (sometimes referred to as catfishing laws),[101] student-athlete NIL (name, image, likeness) laws,[102] digital replica laws, election laws, labor laws, and a host of other AI-specific laws.[103]

---

99. *See, e.g.*, 750 ILL. COMP. STAT. 5/11-23.5 (2024) (criminalizing the "[n]on-consensual dissemination of private sexual images"); TEX. PENAL CODE ANN. § 21.16 (West 2024) (same). Some of these laws expressly cover digital replicas or deepfakes. *See infra* note 103.

100. *See, e.g.*, Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14 *et seq.* (2024); TEX. BUS. & COM. CODE ANN. § 503.001 *et seq.* (West 2024) (limiting capturing and use of biometric identifiers).

101. *See, e.g.*, CAL. PENAL CODE § 528.5 (West 2024) (added in 2011); OKLA. STAT. TIT. 21, § 1450 (2024) (added in 2016); H.B. 783, 89th Leg., Reg. Sess. (Tex. 2025) (law in Texas enacted in 2025 that provides civil liability for "online impersonation").

102. Since 2020, more than thirty states have passed new laws (or amendments to existing ones) that address name, image, and likeness rights for student-athletes. These are often referred to as "NIL" rights even though student-athletes are covered by broader publicity rights that already protect their name, image, and likeness rights. The recent surge in the use of NIL as a term of art has obscured the longstanding existence of such rights. Examples of recently passed bills addressing student athletes include: ARK. ANN. CODE § 4-71-1301 *et seq.* (2024) (providing a specific publicity right for student-athletes and providing some limits on this right) (effective date Jan. 1, 2022); 70 OK. STAT. § 820.21 *et seq.* (2025) (extending NIL rights to student athletes and providing some limits on the right) (effective date May 28, 2021, but amended several times including as recently as May 2025). Several bills have been floated in Congress that would extend federal "name, image, and likeness rights" for college athletes but so far none has passed. *See, e.g.*, The Student Athlete Fairness and Enforcement (SAFE) Act, S. 2932, 119th Cong. (introduced Sept. 29, 2025); College Athlete Economic Freedom Act, H.R.4868, 119th Cong. (introduced Aug. 1, 2025); Student Compensation and Opportunity Through Rights and Endorsements (SCORE) Act, H.R. 4312, 119th Cong. (introduced July 10, 2025). Some of these bills are somewhat strange given that they are drafted as if student-athletes would have no claims under current law, which is not the case. Present Trump recently signed an Executive Order seeking to address the Wild West atmosphere of today's college sports endorsement and payment regime. *See* Exec. Order No. 14,322, 90 Fed. Reg. 35,821 (July 24, 2025) ("Saving College Sports").

103. Some of these laws are general purpose statutes targeting deepfakes across contexts. *See, e.g.*, H.B. 1432, 2024 Sess. (N.H. 2024) (creating a felony if a person knowingly creates, distributes, or presents a deepfake for the purpose of causing financial or reputational harm to another) (effective Jan. 1, 2025). Some laws, while written broadly, have particularly targeted concerns raised by the recording industry. *See, e.g.*, A.B. 1836, 2023–24 Reg. Sess. (Cal. 2024) (enacting protections against digital replicas in amendments to postmortem right of publicity statute, CAL. CIV. CODE § 3344.1 (West 2024)); TENN. CODE ANN. § 47-25-1101 (2024) (adopting ELVIS Act in 2024); LA. REV. STAT. § 51-470.1 et seq. (2025) (adopting broad statutory right of publicity and including consideration of digital replicas).

Other digital replica laws particularly target pornographic contexts or uses that depict intimate parts of a person's body (whether computer-generated or otherwise). *See, e.g.*, CAL. CIV. CODE § 1708.86 (West 2024) (creating civil liability when "an individual . . . appears, as a result of digitization, to be giving a [sexual] performance they did not actually perform or to be performing in an altered depiction") (amended on Oct. 13, 2025 to expand scope to include nudifying, better protect minors, and raise statutory damages to $250,000, see A.B. 621, 2025 Gen. Assemb., Reg. Sess. (Ca. 2025)); 750 ILL. COMP. STAT. 5/11-23.7 (2024) (criminalizing "[n]on-consensual dissemination of sexually explicit digitized depictions") (effective Jan.1, 2025); N.Y. CIV. RIGHTS LAW § 52-C (McKinney 2024) (providing a civil action for circulation of nonconsensual explicit depictions).

Other state laws have targeted deepfakes in the context of elections. *See, e.g.*, CAL. ELEC. CODE § 20010 (West 2024) (making actionable the distribution, "with actual malice," of "materially deceptive" deepfakes "of [a] candidate with the intent to injure the candidate's reputation or to deceive a voter into

Hundreds of these laws have passed in the last five years, making it impossible to encapsulate them here.[104] It is worth highlighting, however, that some of these laws face the same challenges of publicity laws in that many do not focus on regulating public deception and some allow for parties other than the person depicted to authorize deepfakes of that person.

3. General State Laws that Apply to Deepfakes

There are a host of other state-based claims relevant to identity rights that may also apply in some instances of deepfakes. Many of these claims are likely to be successful in the context of regulating deepfakes, particularly claims for the intentional and negligent infliction of emotional distress, defamation, the false light tort, and, as I will discuss further below, unfair competition and trademark laws.

* * *

In short, there are many state laws that already apply to deepfakes, but the sheer number of them and their variations across jurisdictions may be difficult to navigate both for potential plaintiffs and for creators that are trying to stay within the boundaries of the law across jurisdictions.

B. FEDERAL LAWS

There are a number of federal laws, including trademark and copyright laws, that also apply to deepfakes, but not in every instance or for every possible plaintiff. I will consider here both existing laws and some proposed legislation.

Although people are not copyrightable, it is an open question whether a person's digital replica or voice clone could be.[105] Regardless, people can be captured in copyrightable works, and if they retain the copyright in these works or obtain rights (or licenses) to them, then they can use copyright law to restrict unauthorized uses of their images, likeness, performances, and voices that have been captured in these works

---

voting for or against the candidate"); TEX. ELEC. CODE § 255.004(d) (West 2024) (criminalizing creating and distributing "a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality," when the creation and distribution is "with intent to injure a candidate or influence the result of an election").

Several states have adopted new laws or amended their employment and labor laws to regulate contracts for the creation and use of digital replicas. *See, e.g.*, CAL. LAB. CODE § 927 (West 2024); Public Act 104-0282 (Ill. 2024); N.Y. GEN. OBLIG. LAW § 5-302 (McKinney 2024). New York recently adopted a law requiring advertisers to disclose when a digitally created "synthetic performer" is used in advertisements. *See* S.8420-A/A.8887-B, 2025–2026 Reg. Sess. (N.Y. 2025) (signed into law December 11, 2025).

104. *See, e.g., supra* notes 99–103; *see also* Thomas E. Kadri & Sonja R. West, *Deepfake Torts: Emerging Torts Frameworks in the U.S. Deepfake Regulation*, 18 J. TORT L. 515, 518–19 (2025) (documenting 122 new deepfake laws passed during the period between January 2023 and May 2025, and 344 proposed laws related to regulating deepfakes).

105. *See* Rothman, *supra* note 61.

and the creation of derivatives based on them.[106] There are a number of cases currently being litigated to determine the ability of copyright law to limit the creation of digital replicas and voice clones, but they are still in the early stages or have settled, leaving the legal questions unanswered.[107]

Unfair competition and trademark laws both at the state and federal level also protect against unauthorized uses of a person's identity, most often uses of a person's name or likeness, but also voice.[108] These laws protect individuals by restricting the unauthorized use of a person's identity as a mark (or otherwise) to falsely indicate source, endorsement, or sponsorship and in some instances to prevent the dilution of a famous "personal mark."[109] Such claims are usually limited to those that arise from using the identity of a person who sells goods or services associated with their identity. State and federal consumer protection laws and regulations also limit unauthorized uses of a person's identity, as do laws prohibiting fraud and false advertising.

In contrast to right of publicity claims, all of these claims (other than dilution) require a demonstration of likely confusion of consumers. These unfair competition

106. *See, e.g.*, Balsley v. LFP, Inc., 691 F.3d 747 (6th Cir. 2012) (using copyright to limit circulation of plaintiff in wet t-shirt contest); Monge v. Maya Magazines, Inc., 688 F.3d 1164, 1184 (9th Cir. 2012) (copyright limited unauthorized circulation of wedding photos); Michaels v. Internet Ent. Grp., Inc., 5 F. Supp. 2d 823 (C.D. Cal. 1998) (using copyright to limit circulation of sex tape); *see also* Shyamkrishna Balganesh, *Privative Copyright*, 73 VAND. L. REV. 1, 4–5 (2020); Rothman, *supra* note 61, at 18–24.

107. *See, e.g.*, Lerhman v. Lovo, Inc., 790 F. Supp. 3d 348 (S.D.N.Y. 2025) (allowing right of publicity claims to proceed and leave to amend copyright claims arising out of unauthorized use of plaintiffs' voices in AI-generated voice clones); Complaint at 23–25, UMG Recordings, Inc. v. Suno, Inc., No. 24-11611, 2025 WL 3524289 (D. Mass., filed June 24, 2024) (contending that AI-generated songs violate copyright in recordings in part on basis of use of performers' voices); Complaint, UMG Recordings, Inc. v. Uncharted Labs, Inc., No. 24-04777, 2025 WL 1047517 (S.D.N.Y., filed June 25, 2024) (objecting to use of recording artists' "vocal style" from copyrighted recordings in AI-generated output, including outputs similar to Mariah Carey, Bruce Springsteen, and Frank Sinatra); *cf.* Order Denying Motion to Dismiss, Concord Music Grp., Inc. v. Anthropic PBC, No. 24-03811-EKL, (N.D. Cal. Oct. 6, 2025) (allowing copyright claims to proceed arising out of use of song lyrics in training AI models and their outputs). Several of the lawsuits brought by record labels have settled. Notably, the settlements have involved partnerships to create AI-generated music with the defendants rather than to limit their actions. *See, e.g.*, Stipulation of Dismissal, UMG Recordings, Inc. v. Suno, Inc., No. 24-11611 (D. Mass., filed Jan. 28, 2026) (dismissing case brought by Atlantic Records, Rhino Entertainment, Warner Music, and others); Stipulation of Dismissal by Plaintiffs UMG Recordings, Inc., and Capitol Records, LLC, No. 24-04777 (S.D.N.Y., filed Nov. 5, 2025); Stipulation of Dismissal by Plaintiffs Atlantic Recording Corp. et al., LLC, No. 24-04777 (S.D.N.Y., filed Nov. 5, 2025) (dismissing case brought by Warner Music, Rhino Entertainment, and others); *Warner Music Group, Udio Settle Copyright Case, Plan New AI Song Creation Platform*, REUTERS (Nov. 19, 2025), https://www.reuters.com/legal/litigation/warner-music-settles-with-ai-firm-udio-plans-joint-platform-2025-11-19/; Press Release, Warner Music Group, Warner Music Group and Suno Forge Groundbreaking Partnership (Nov. 25, 2025), https://www.wmg.com/news/warner-music-group-and-suno-forge-groundbreaking-partnership [https://perma.cc/T266-KT77].

108. *See* Rothman, *supra* note 19, 1278–79; *see also* Rachel Buckland & Shivani Chelliah, *Much Ado About McConaughey*, ROTHMAN'S ROADMAP (Feb, 27, 2026), https://rightofpublicityroadmap.com/news_commentary/much-ado-about-mcconaughey/ [https://web.archive.org/web/20260323224332/https://rightofpublicityroadmap.com/news_commentary/much-ado-about-mcconaughey/] (analyzing recent press coverage of actor's trademark registrations given long history of personal marks, including their registration at the USPTO).

109. "Personal marks are those that include (or are entirely composed of) the portrait, name, or other indicia of identity of a natural person." Rothman, *supra* note 19, at 1276.

laws could help combat public deception to some degree in the context of deepfakes, but not entirely; the focus of the deception inquiry in these laws is usually on confusion as to source, sponsorship, or affiliation rather than on whether the public is deceived into thinking a deepfake is an authentic recording. Additionally, such laws will usually not provide claims for those whose identities do not have commercial value.

Congress has also recently passed and is considering passing other laws that address certain aspects of name, image, likeness and voice rights.[110] The Take It Down Act recently signed into law by President Trump facilitates the removal from online platforms of unauthorized intimate visual depictions, including AI-generated ones.[111] Of the many other bills being floated to address deepfakes, the NO FAKES Act thus far appears to have the most support of these proposed bills. The title is short for "Nurture Originals, Foster Art, and Keep Entertainment Safe Act." The title itself highlights that this was drafted with the entertainment industries in mind, even though it would apply to everyone. The bill would create a federal digital replica right, including a postmortem right, and create liability for producing, publishing, reproducing, displaying, distributing, transmitting or "otherwise making available to the public" a digital replica.[112] It provides statutory damages ranging from $5,000 to $25,000 for entities that are not online service providers.[113] The bill would allow for some reuse of copyrighted works (including sampling, remixing, and remastering, and reuse of some performances if they are not "fundamentally" or "materially altered").[114]

The bill runs thirty-nine pages—and is still a work-in-progress. In the context of our symposium's topic of deepfakes, I want to therefore focus on how the proposed NO FAKES Act would address the key concerns that we identified arising out of deepfakes that center on authorization and deception. The short answer is that it doesn't do a good job of addressing either concern. First, it says nothing about addressing public deception and may increase the number of deceptive deepfakes by further incentivizing a market for them. Second, the bill doesn't protect against deceptively-authorized deepfakes—remember, those are the deepfakes that might technically be authorized as a legal matter but that are not in fact specifically known or approved by the identity-holder. This is so because the bill allows long-term, broad licensing with insufficient guardrails and allows authorized representatives to enter such licensing agreements without consulting the identity-holder.[115] As the bill is redrafted, deception and

110. *See, e.g.*, Take It Down Act, Pub. L. No. 119-12, 139 Stat. 55 (2025) (codified as amended at 47 U.S.C. §§ 223–223a); NO FAKES Act of 2025, *supra* note 6; *see also* No AI FRAUD Act of 2024, *supra* note 48; PADRA, *supra* note 6.

111. Take It Down Act, *supra* note 110. Notably, a district court has recently called into question the law's effectiveness by suggesting that § 230 of the Communications Decency Act blocks platform liability. Doe v. X Corp., No. 4:25-cv-01282-0, at 11–12 (N.D. Tex. 2026).

112. NO FAKES ACT of 2025, *supra* note 6.

113. *Id.* § 2(e)(4).

114. *Id.* § 2(a)(2).

115. Although the bill requires that licenses identify the uses to be exercised with a "reasonably specific description," this does not require the person's actual knowledge and it is not clear how even this proposed limitation would be interpreted. For example, would a description of the use of a person's digital replica as "in audio-visual works" be "reasonably specific"? Would uses in promotions for a particular brand of soda or

authorization should be at the center of the drafting rather than profit-maximization for third parties and immunization for internet platforms.

* * *

In sum, even though we have many—maybe too many—overlapping and sometimes conflicting laws in the United States that address deepfakes, they frequently do not keep their eye on the key dangers. Often both the laws on the books (and those being proposed) do not adequately focus on whether the deepfakes are authorized by those depicted and/or whether the deepfakes deceive the public as to their authenticity.[116] The current explosion in overlapping laws that all extend rights or claims based on the attributes of a real person have also exacerbated what I elsewhere have dubbed an "identity thicket," further complicating the navigation of the legal landscape covering deepfakes.[117] Ideally, any new federal laws would try to thin out the "identity thicket" rather than worsen it.

V. CONCLUSION

With all of this discussion of the law, it's important to note that law alone cannot combat deepfakes. We will need to work with technologists to build guardrails against the creation and dissemination of unauthorized and deceptive deepfakes. We need tools to prove authenticity and to detect fakes. Laws can be designed to encourage such private sector efforts but at the federal level this has not been the focus. Some states, particularly California, however, have tried to do this and we will have to see how successful these efforts are. Requiring platforms to address deepfakes is also essential since having laws on the books that are hard to or impossible to enforce will have little impact.

We also do not know how the market will react to this era of deepfakes. For example, we may find that people will crave authentic performances, perhaps reviving live theater and preferring DJ-moderated, human-created music to AI-generated playlists filled with fake recordings by fictional artists. Certification regimes that mark things as human-made, among other market-driven approaches, could help support these consumer choices.

In our rush to fix the problem of deepfakes, we should make sure that the law does not worsen the problem by giving legitimacy to deceptively-authorized deepfakes. Nor

apparel be "reasonably specific"? The limitation is essentially useless if both of these examples count. For consideration of these and other concerns with the current draft of the NO FAKES Act, see Rothman, *Still Needs Revision*, *supra* note 47.

116. Addressing these crucial concerns at the same time and across contexts would have the added benefit of reducing the underinclusivity concerns of more targeted approaches. See discussion *supra* note 31 and accompanying text. It could also highlight alternatives to mandated disclosures that may be struck down as compelled speech or that may have limited effectiveness. *See* Nat'l Inst. of Family & Life Advocates v. Becerra, 585 U.S. 755 (2018) (holding that state's notice requirement for crisis pregnancy centers is likely unconstitutional).

117. Rothman, *supra* note 19, at 1273, 1278–89.

should the law overlook the harms that flow from even authorized deepfakes that deceive the public. Unfortunately, too much of the recently proposed and enacted legislation does exactly this. Given that we already have many laws at both the state and federal level that apply to deepfakes, further legislation in this area should be squarely focused on addressing the current gaps in the law, with an eye toward limiting deceptive uses and ensuring that the people depicted truly agreed to the deepfake portrayal.