VOLUME 6 July 2025 ISSUE 2

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

STATES LEGISLATING AGAINST DIGITAL DECEPTION: A COMPARATIVE STUDY OF LAWS TO MITIGATE DEEPFAKE RISKS IN AMERICAN POLITICAL ADVERTISEMENTS

HAYDEN GOLDBERG

Abstract

This article asks two questions. First, "are recently passed bills prohibiting unlabeled deepfakes in campaign advertisements necessary?" To answer this question, I ask "what risks do legislators envision new and old laws addressing?" For new laws, I transcribe their statements in committee hearings and conduct a qualitative thematic analysis to develop risk models. For old laws, I draw on hearings and case law. I find legislators envision new laws address risks regarding election security, their own reputation, and information. Informational risks' constituent components are the right to access true information, the right to know something has been manipulated, the risk of false/deceptive information, and an obligation for campaigns to be truthful. In contrast, I find that the risks older laws address concern voter suppression or intimidation, the risks of the undermining of civil rights, or fraudulent fundraising tactics. I argue these laws are inadequate for addressing new risks because they are intended to cover vastly different actions. In contrast, existing state laws prohibiting candidates representing themselves certain ways have partial overlap with risk models for new laws, but fail to cover all types of misrepresentations, demonstrating the new for new laws. Therefore, I conclude that the risks deepfakes present are a difference of kind of risk, not a difference in degree. This limits the

utility of existing laws, demonstrating the necessity of new ones. By systematically demonstrating the shortcoming of existing laws, I provide insight into law and technology, election law, and the study of deepfake risks.

States Legislating Against Digital Deception: A Comparative Study of Laws to Mitigate Deepfake Risks in American Political Advertisements

HAYDEN GOLDBERG[*]

INTRODUCTION

Scholars have long debated whether new laws are needed to address new technologies and their risks, or if existing laws suffice.[1] In the digital technology space, this debate appears in research on search engines, data protection, algorithmically defined groups, and antitrust.[2] Deepfakes are an emerging technological innovation with disruptive potential. They are computer-generated videos, audio clips, or images purporting to represent someone saying or doing something that did not occur in reality.[3] They could potentially massively shift the information

[*] For guidance on this project, I thank Prof. Sandra Wachter. Shanell Logan, Will Shao, Gwendoline Palmer-Steeds, Emelie Lindow, Cassidy Bereskin, Ingrid Epure, Will Hale, Jack Jacobs, Diego Ramirez Alcade, Gillian Diebold, Hannah Lederman, and Jess Miller provided useful feedback. Professors Spencer Overton, Rebecca Green, Rick Hasen, Nate Persily, and Tobin Raju provided valuable advice. This project would not have been possible without the help of legislative librarians and staff, including Jillian Slaight, Bryce Grunwaldt, Lori Barber, Ethan Jones, Garrett Shields, Elizabeth Hinderer, Melanie Harshman, Corbin Heinchon, Stephen Parks, John Cannon, Michelle Diffin, Kyle Slominski, Jeffrey Buckley, Emily Donnellan, Joanne Montague, Janice Selberg, and Rachel Clark.

[1] *See, e.g.,* Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. ILL. J. L. TECH. & POL'Y 239, 238–241 (2007) (discussing the impact of changes in railroads, genetic testing, and computers on the law).

[2] *See, e.g.,* Oren Bracha & Frank Pasquale, *Federal Search Commission - Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008) (arguing search engines limit the open exchange of ideas by suppressing speech but could be regulated without running afoul of the First Amendment); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2015) (arguing fiduciary duties should apply to technology companies that collect data); Sandra Wachter, *The Theory of Artificial Immutability: Protecting Algorithmic Groups under Anti-Discrimination Law*, 97 TUL. L. REV. 149 (2022) (asking if non-discrimination law can be used to regulate algorithmically defined groups); Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L. J. 710 (2017) (arguing contemporary anti-trust regulations are inadequate to deal with modern firms like Amazon).

[3] *See* Robert Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1758–1759 (2019).

environment in elections, which is concerning for voters and the public.[4]

However, as new regulation in this space is proposed, it is worth stepping back and asking if this legislation is necessary. To do so, this article asks three questions:

- RQ1: Are new laws prohibiting deepfakes in political advertisements necessary?
- RQ2: What risks of deepfakes do legislators envision when passing laws prohibiting deepfakes in campaign ads?
- RQ3: What risks are addressed by existing laws which may be used to prohibit deepfakes in campaign ads?

Passing new laws indicates states envision a gap in the law where the harms of deepfakes are inadequately addressed. Ensuring injuries have a remedy is a critical tenet of common law, yet scholarly literature has inadequately assessed if existing laws could mitigate election-related deepfake risks.[5] This article seeks to fill this gap by looking at legislator's commentary and case law to understand the intended scope and application of new and existing laws. This is the work of Parts III and IV, which articulate theoretical "risk models." Then I compare the models to answer RQ1.

I argue old laws address five types of risk: voter intimidation, conspiracies to undermine rights, robocalls, fraudulent misrepresentations, and impediments to giving support or advocacy for federal candidates. Two upcoming decisions will be crucial to determining if a subset of these laws can apply to deepfakes. Meanwhile, committee hearings on new laws reveal legislators intended the laws to address risks concerning election security, candidate reputations, and the information environment. Then I analyze the text of the laws to understand the legal mechanisms being used to address these risks. I argue deepfake laws enact different legal philosophies via differences in who can be injured, the role of intent, and different behavioral outcomes.

Overlaying the two risk models, I answer RQ1 and argue the laws

---

[4] *See, e.g.,* Candidate 1083032, Subversive Technologies Summative Paper (2024) (Seminar paper, University of Oxford) (on file with the author) (arguing deepfakes are a negative externality on the information environment); Morgan Meaker, *Slovakia's Election Deepfakes Show AI Is a Danger to Democracy*, WIRED (Oct. 3, 2023), https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/ (discussing a deepfake released of a presidential candidate hours before the election and during a media moratorium).

[5] *See, e.g.,* Note, *Developments in the Law — Injunctions*, 78 HARV. L. REV. 994 (1965) (discussing the role of injunction as one particular type of remedy in the common law context).

reflect differences in kind of risk, not of degree.[6] New laws are candidate and information-centric, while old laws center on effectuating voting rights. The most overlap between the models is found with fraudulent misrepresentations and deceptive injuries, which both concern how voters perceive candidates.

This article proceeds as follows. Part I reviews the literature on deepfakes and their risks, focusing specifically on electoral risks.[7] Additionally, it reviews scholarship on deepfakes. Part II provides the methodology used to acquire, transcribe, and analyze testimony on new and old laws. Part III answers RQ3, Part IV addresses RQ2, and Part V brings these pieces together to answer RQ1. Finally, Part VI brings together lessons from the risk models to inform future legislation.

I. Literature Review

This article intersects a multidisciplinary literature regarding deepfakes, free speech, and election law. Accordingly, I first review deepfakes in general, discussing how they impact the information environment; I do not provide a technical overview.[8] Second, I review the risks AI and deepfakes specifically are posing to elections. Throughout these sections, special attention is given to the election risk, as this contextualizes the risks new laws seek to address. Finally, I review the legal context, including campaign finance regulation, the "right to lie" in political campaigns, the legal implications of deepfakes, and legal scholarship specifically examining deepfakes and elections.

A. Deepfakes

One form of artificial intelligence ("AI") is deepfakes. Deepfakes are artificially generated images, audio, or video purporting to

---

[6] This language borrows from Animal Legal Def. Fund v. Herbert, 263 F. Supp. 3d 1193, 1210 (D. Utah 2017).

[7] I do not address other risks or harms like deepfake pornography and the impact deepfakes have on legal evidence. For a review of these topics, *see, e.g.*, Danielle Keats Citron, *Sexual Privacy*, 128 YALE L. J. 1870, 1921–1924 (2019) (arguing deepfake pornography is a privacy violation); Riana Pfefferkorn, *"Deepfakes" in the Courtroom*, 29 B.U. PUB. INT. L. J. 245 (2020) (discussing evidentiary challenges introduced by deepfakes); *cf.* Natasha Singer, *Teen Girls Confront an Epidemic of Deepfake Nudes in Schools*, N.Y. TIMES (Apr. 8, 2024), https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html (discussing how American schools are taking different approaches to reporting deepfake pornography).

[8] For a review of key technical papers, *see* Anukriti Kaushal et al., *A Review on Deepfake Generation and Detection: Bibliometric Analysis*, MULTIMEDIA TOOLS & APPLICATIONS, 87582–85 tbl.1 (2024).

demonstrate a person saying or doing something they did not do in reality.[9] Created using generative adversarial networks, these are a type of generative AI which is trained on imagery of someone and can replicate their likeness, including voice and facial expressions. [10] Deepfakes only need to be trained on a small selection of records or images of a person before being able to be produced.[11] Despite deepfakes all using the same underlying technology, a recent systematic review found there was no universal definition of deepfakes in the scholarly literature; definitions varied based on technology and output medium.[12] This is indicative of my finding that definitions vary among states.

Robert Chesney and Daniel Keats Citron wrote the first major paper exploring the harms of deepfakes.[13] They emphasize the breadth of risks deepfakes present, including harms to individuals, groups, or society at large depending on how they are used.[14] Harms occur because a deepfake purports to be a truthful representation of reality, tricking people into thinking it is real when it is not.[15] This includes the Liar's Dividend, a harm occurring when deepfakes are used to deny something occurred.[16]

Deepfakes harm the information environment by 1) making people question the content in front of them and 2) increasing the amount of disinformation people see. Prior work theorized the latter as information environment harm, creating negative externalities labeling mitigates. [17] In the current information paradigm, photo or video evidence "is what the proponent claims it is," but deepfakes undermine this. [18] "Seeing is no longer believing," creating challenges for issues ranging from how people respond to videos about themselves to how

---

[9] *See* Chesney & Citron, *supra* note 3, at 1758.
[10] *See, e.g.*, Supasorn Suwajanakorn et al., *Synthesizing Obama: Learning Lip Sync from Audio*, 36.4 ACM TRANSACTIONS ON GRAPHICS 1, 2 (2017).
[11] *See* Hany Farid, *Creating, Using, Misusing, and Detecting Deep Fakes*, 1.4 J. ONLINE TR. & SAFETY 1, 2–7 (2022) (discussing the necessary data to create audio, photograph, and video deepfakes).
[12] *See* Alena Birrer & Natascha Just, *What We Know and Don't Know About Deepfakes: An Investigation into the State of the Research and Regulatory Landscape*, NEW MEDIA & SOC'Y 5 (2024) ("There is, however, no universally accepted definition and studies diverge[] in their interpretation of common conceptual elements.").
[13] *See* Chesney & Citron, *supra* note 3, at 1771–85.
[14] *Id.* at 1771–85.
[15] *Id.* at 1785; *cf.* Don Fallis, *The Epistemic Threat of Deepfakes*, 34 PHIL. & TECH. 623, 625 (2021) ("The main epistemic threat is that deepfakes can easily lead people to acquire false beliefs. That is, people might take deepfakes to be genuine videos and believe that what they depict actually occurred.").
[16] Chesney & Citron, *supra* note 3, at 1785.
[17] *See* Candidate 1083032, *supra* note 4.
[18] FED R. EVID. 901(a).

evidence is evaluated in court.[19]

B. AI and Elections

Scholars have articulated numerous real and imagined risks of AI and deepfakes, such as their potential to harm the electoral ecosystem. These likely inform the public narrative around deepfakes, and therefore legislative testimony articulating risks.

At a high level, Chesney and Citron's discussion on risks foregrounds a larger discussion about the pros and cons of AI in elections. Political communications researcher Andreas Jungherr suggests considering AI's impacts on election-related topics like news, the information environment, and persuasion to better articulate its potential impact.[20] Despite that, he argues, "AI is unlikely to impact many aspects of democracy directly," but notes its perceived effects are almost as important as its actual effects.[21] Therefore, analyses must consider its potential effects, especially since legislators – the primary actor studied here – speak with rhetorical ethos giving significant persuasive power to shift the public's mindset.

AI can be used for good and for ill in elections. Most scholarship picks one side of this binary, risking falling into a trap of techno-determinism and techno-optimism.[22] Optimists claim algorithms could partially automate election administration processes like voter roll maintenance and signature verification.[23] Pessimists explore how AI could undermine the rule or law or shift public opinion.[24] Generative AI could assist politicians in reaching new audiences, engaging members of

---

[19] *See, e.g.*, Regina Rina & Leah Cohen, *Deepfakes, Deep Harms*, 22 J. ETHICS & SOC. PHIL. 143, 157 (2022) (arguing there are three harms when people see videos of themselves: virtual domination, illocutionary harms, and panoptic gaslighting); Pfefferkorn, *supra* note 7 (discussing how evidence should be used in court and what tools are available to mitigate these harms).

[20] *See* Andreas Jungherr, *Artificial Intelligence and Democracy: A Conceptual Framework*, 9 SOC. MEDIA & SOC'Y 1, 4–5 (2023).

[21] *Id.* at 9.

[22] *Compare* Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J. L. & TECH. 106, 149 (2019) (pessimistic), *with* Deepak P. et al., *AI and Core Electoral Processes: Mapping the Horizons*, 44 AI MAG. 218, 220 (2023) (optimistic). *But see* Prathm Juneja, *Artificial Intelligence for Electoral Management,* INT'L IDEA 7 (2024), https://doi.org/10.31752/idea.2024.31 (balanced approach).

[23] Sarah M. L. Bender, *Algorithmic Elections*, 121 MICH. L. REV. 489, 502–510 (2022).

[24] *See, e.g.*, Manheim & Kaplan, *supra* note 22, at 112.

a language minority, and overcoming language barriers.[25] Expanding on this point, Professor Spencer Overton recently postulated race-based discriminatory harms, arguing they can exacerbate existing inequalities by targeting attacks and disproportionately harming minority communities.[26] This joins a growing literature critiquing algorithmic-based systems for their discriminatory harms.[27] Both Overton and William Marshall have made innovative arguments to apply old laws to hold perpetrators accountable for harmful democratic discourse in areas traditionally protected by liability shields.[28] I follow their approach of finding ways to regulate generally-protected political speech, but use different laws.

Following Jungherr's call, a burgeoning literature investigates if there is empirical grounding to fears AI could be used for persuasion. One study found deepfakes decreased certainty in the truthfulness of the content, reducing people's trust in the media.[29] Two recent papers demonstrate large language models can be persuasive when making personalized political *ads*, but the efficacy of personalized political *messaging* is not statistically significantly different from non-personalized messaging.[30] A political science study found distorting an opposing party's message was effective, even accounting for partisan-

---

[25] Emma G. Fitzsimmons & Jeffery C. Mays, *Since When Does Eric Adams Speak Spanish, Yiddish and Mandarin?*, N.Y. TIMES (Oct. 20, 2023), https://www.nytimes.com/2023/10/20/nyregion/ai-robocalls-eric-adams.html (describing the use of deepfakes in different languages to reach voters).

[26] *See* Spencer Overton, *Overcoming Racial Harms to Democracy from Artificial Intelligence*, 110 IOWA L. REV. 805, 833 (2025).

[27] *See*, *e.g.*, Wachter, *supra* note 2; Nithya Sambasivan et al., *Re-Imagining Algorithmic Fairness in India and Beyond*, *in* FACCT '21: PROCEEDINGS OF THE 2021 ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 315 (2021); Sandra Wachter et al., *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, 41 COMPUT. L. & SEC. REV. 1, 2 (2021); Brent Mittelstadt, *From Individual to Group Privacy in Big Data Analytics*, 30 PHIL. & TECH. 475 (2017).

[28] *See* Spencer Overton, *State Power to Regulate Social Media Companies to Prevent Voter Suppression*, 53 U.C. DAVIS L. REV. 1793 (2020); William P. Marshall, *Internet Service Provider Liability for Disseminating False Information about Voting Requirements and Procedures*, 16 OHIO ST. TECH. L. J. 669, 689–94 (2020).

[29] *See* Cristian Vaccari & Andrew Chadwick, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*, 6 SOC. MEDIA & SOC'Y 1, 2 (2020) ("[While] we do not find evidence that deceptive political deepfakes misled our participants, they left many of them uncertain about the truthfulness of their content. And, in turn, we show that uncertainty of this kind results in lower levels of trust in news on social media.").

[30] *See* Almog Simchon et al., *The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence*, 3 PROC. NAT'L ACAD. SCI. NEXUS 1 (2024) (personalized ads); Kobi Hackenburg & Helen Margetts, *Evaluating the Persuasive Influence of Political Microtargeting with Large Language Models*, 121 PROC. NAT'L ACAD. SCI. 1 (2024) (personalized messages).

motivated reasoning.[31] These studies lend empirical support to the claim personalized AI-generated content, and/or deepfakes, can persuade, deceive, or change people's voting behavior.[32] However, it is important to remain skeptical of personalization because more research is needed.[33]

Deepfakes are new and transform the information paradigm by changing the notion of truth and the believability of evidence.[34] The *potential* for audio and visual media to be a deepfake is a central harm.[35] This creates a concerning paradigm shift; some scholars argue the *fear* of other harms being realized is the biggest harm.[36]

Other scholars have narrowly considered threats to the information environment, arguing deepfakes decrease democratic functions and norms by weakening news media and impeding citizens' ability to engage in debate.[37] This decreases democratic legitimacy by undermining the quality of civic debate.[38] The information environment risks I identify below explicitly articulate this risk. Finally, a categorization of campaign-specific harms shifted attention to actors, motivations, modalities, campaign phases, distribution channels, and mechanisms for influencing voters.[39] This approach rightly emphasizes how the effect deepfakes have depends on their content and who releases

---

[31] *See* Zeynep Somer-Topcu & Margit Tavits, *Message Distortion as a Campaign Strategy: Does Rival Party Distortion of Focal Party Position Affect Voters?*, 85 J. POL. 892 (2023).

[32] *See also* Kaylyn Jackson Schiff et al., *The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability?*, AM. POL. SCI. REV. 1, 3 (2024) (finding that when a mock candidate invokes the Liar's Dividend the dividend is effective for candidates seeking to discredit text-based information about them, but not video-based evidence).

[33] *See*, *e.g.*, Hannah Rose Kirk et al., *The Benefits, Risks and Bounds of Personalizing the Alignment of Large Language Models to Individuals*, 6 NATURE MACH. INTEL. 383 (2024).

[34] *See*, *e.g.*, Fallis, *supra* note 15, at 625 (arguing "[t]he main epistemic threat is that deepfakes can easily lead people to acquire false beliefs. That is, people might take deepfakes to be genuine videos and believe that what they depict actually occurred.").

[35] While this is primarily a theoretical conclusion, it is backed up by empirical evidence. *See*, *e.g.*, Vaccari & Chadwick, *supra* note 29.

[36] *See*, *e.g.*, Maria Pawelec, *Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions*, 1 DIGIT. SOC'Y 1, 14–15 (2022) ("Importantly, however, deepfakes have caused great concern among academia, journalists, political actors, and, increasingly, the public. I argue that this fear itself—rather than deepfakes' actual use in elections—currently constitutes electoral deepfakes' greatest threat to democracy: It undermines citizens' and other political stakeholders' trust in the fairness and integrity of elections. Thus, it fuels societal trust decay.") (internal citations omitted).

[37] *See id.* at 23.

[38] *See id.*

[39] *See* Nicholas Diakopoulos & Deborah Johnson, *Anticipating and Addressing the Ethical Implications of Deepfakes in the Context of Elections*, 23 NEW MEDIA & SOC'Y 2072, 2076 (2020).

them. Thus, risk models can be understood as a series of sliding scales, with each scale being a different feature.

Finally, there are two harms voters may experience. First, deepfakes could sway an election at the last minute, like what happened during the media moratorium preceding the 2023 Slovakian election.[40] Second, scholars fear deepfakes could subtly be inserted into our information streams and sway public opinion, akin to Russian disinformation in 2016.[41]

C. Election Law

The following discussion on (election) law focuses on campaign finance law, lying in elections, the legal implications of deepfakes, and legal scholarship on deepfakes in elections.

1. Campaign Finance Law

The state laws examined below concern requirements for disclosures on campaign ads. These requirements have broadly been upheld.[42] They have two main elements: contribution and expenditure reporting, and "paid for by" disclaimers on ads.[43] Disclosure may incentivize firms to conceal the true source of funding by using intermediaries.[44] This claim is bolstered by empirical work showing disclosure about the origins of political advertising changes voting

---

[40] *See, e.g.*, Meaker, *supra* note 4 (describing how an audio deepfake was released during the moratorium on news coverage in the 48 hours before Slovakian elections).
[41] *See, e.g.*, *Advances in Deepfake Technology: Hearing Before the Subcomm. on Cybersecurity, Info. Tech., and Gov't Innovation of the Comm. on Oversight & Accountability*, 118th Cong. 11 (2023) (testimony of Spencer Overton, Professor of L., Geo. Wash. U., at 11) ("So, when we think back to 2016, the Russians, we know, set up social media accounts pretending to be Black Americans . . . Now today, in this world, the Russians or domestic bad actors could spark social upheaval by creating deepfake videos.").
[42] For a historical overview, *see* Abby K. Wood, *Campaign Finance Disclosure*, 14 ANN. REV. L. & SOC. SCI. 11 (2018).
[43] *See id.* at 13 ("Campaign finance disclosure usually refers to two activities: disclosure and disclaimers . . .Campaign finance disclosure is conducted via reporting obligations, with periodic deadlines that increase in frequency as the election approaches . . . Campaign finance disclaimers are the 'stand by your ad' requirements that appear with political messages. They identify the entity that paid for the ad.").
[44] *See* Citizens United v. Fed. Election Comm'n., 558 U.S. 310, 459–460 (2010) (Stevens, J. concurring in part and dissenting in part) ("It underscores that for-profit corporations associated with electioneering communications will often prefer to use nonprofit conduits with 'misleading names,' such as And For The Sake Of The Kids, 'to conceal their identity' as the sponsor of those communications, thereby frustrating the utility of disclosure laws.") (internal citations omitted).

behavior.[45] Concealing the identity of the creator to obfuscate the true origin and motives is a potential harm of deepfakes.

The Supreme Court has upheld mandated financial disclosures.[46] The Court has held that the Internet increases the efficacy of disclosure by lowering barriers to accessing information. [47] These holdings emphasize how digitalization of disclosure makes it possible for the public to quickly learn about the origins of an ad, thereby reducing the appearance of corruption and "fostering an informed electorate."[48] The same logic applies to new disclosure laws: by informing people if an ad contains a deepfake, the state is increasing the public's awareness of the campaign.

2. The Right to Lie and United States v. Alvarez

United States v. Alvarez is a 2012 Supreme Court decision which has been interpreted as establishing a "right to lie" in elections.[49] This decision contextualizes the new laws because they seek to regulate, but not prohibit, false election speech. Below, I argue state laws are narrowly scoped to comply with *Alvarez*.[50]

On First Amendment grounds, Xavier Alvarez appealed his

---

[45] *See*, *e.g.*, Abby K. Wood & Douglas M. Spencer, *In the Shadows of Sunlight: The Effects of Transparency on State Political Campaigns*, 15 ELECTION L. J. 302, 315 (2016) ("Our findings indicate that disclosure, particularly in the form of increased visibility of contributions, has a negligible deterrent effect on contributors."); Abby K. Wood, *Learning from Campaign Finance Information*, 70 EMORY L. J. 1091, 1142 (2021) (reviewing the existing literature on campaign finance disclosure and "suggest[ing] that the current framework short sells the informational benefit of campaign finance disclosure, and that voters punish dark money and reward transparency.").

[46] *See* Buckley v. Valeo, 424 U.S. 1 (1976) (per curiam).

[47] *See* McCutcheon v. Fed. Election Comm'n, 572 U.S. 185, 224 (2013) ("With modern technology, disclosure now offers a particularly effective means of arming the voting public with information. In 1976, the Court observed that Congress could regard disclosure as 'only a partial measure.' That perception was understandable in a world in which information about campaign contributions was filed at FEC offices and was therefore virtually inaccessible to the average member of the public. Today, given the Internet, disclosure offers much more robust protections against corruption. Reports and databases are available on the FEC's Web site almost immediately after they are filed . . . Because massive quantities of information can be accessed at the click of a mouse, disclosure is effective to a degree not possible at the time *Buckley*, or even *McConnell*, was decided.") (internal citations omitted).

[48] *See* Eu v. S.F. Democratic Cent. Comm., 489 U.S. 214, 228–29 (1989) ("[California argues] it is necessary to protect primary voters from confusion and undue influence. Certainly the State has a legitimate interest in fostering an informed electorate . . . a State may regulate the flow of information between political associations and their members when necessary to prevent fraud and corruption.").

[49] *See* United States v. Alvarez, 567 U.S. 709 (2012).

[50] *See infra* § V.

conviction for violating the Stolen Valor Act. It prohibited falsely representing oneself as a winner of military medals. He "challenge[d] the statute as a content-based suppression of pure speech," while "[t]he Government defend[ed] the statute as necessary to preserve the integrity and purpose of the Medal [in question]," which, "it contend[ed]," his lies "frustrated."[51]

The highly splintered decision had three opinions, each with a unique approach. The plurality used strict scrutiny while the concurrence used intermediate scrutiny. While the plurality and concurrence were focused on overbreadth concerns – and thus conducted a scrutiny-based analysis – Justice Alito's dissent emphasized the value of this false speech. He reasoned Alvarez's speech was valueless, and the statute was narrowly tailored, so he would have upheld the law.

Plurality opinions bind lower courts.[52] However, *Alvarez* is difficult to parse because "the disagreement among Justices is one of kind—whether to apply strict or proportional scrutiny—not of breadth."[53] That is, the standard it enacts is unclear – a problem of "kind" – not a question of which portion of potentially applicable cases it should apply to.

Scholars and courts broadly agree the Supreme Court rejected the United States' argument that lies are categorically unprotected speech.[54] That is, false speech is *not* categorically unprotected, like obscenity or fighting words.[55] This is known as "the right to lie."[56]

---

[51] *Alvarez*, 567 U.S.at 715 (Kennedy, J.) (plurality opinion).

[52] *See* Marks v. United States, 430 U.S. 188 (1977) ("When a fragmented Court decides a case . . . 'the holding of the Court may be viewed as that position taken by those Members who concurred in the judgments on the narrowest grounds.'") (quoting *Gregg v. Georgia*, 428 U.S. 153, 169 n.15 (1976)).

[53] *Animal Legal Def. Fund*, 263 F. Supp. 3d at1210.

[54] *Alvarez*, 567 at 719 (holding that the Supreme Court, "has never endorsed the categorical rule the government advances: that false statements receive no First Amendment protection . . . moreover, the Court has been careful to instruct that falsity alone may not suffice to bring the speech outside the First Amendment"); *id.* at 732–33 (Breyer, J. concurring in judgment) ("[T]his Court has frequently said or implied that false factual statements enjoy little First Amendment protection. But these judicial statements cannot be read to mean 'no protection at all.'") (internal citations and quotations omitted).

[55] *See, e.g.,* People for the Ethical Treatment of Animals, Inc. v. N.C. Farm Bureau Fed'n, Inc., 60 F.4th 815, 836 n.8 (2023) (interpreting *Alvarez* as "declining to hold broadly that all 'false statements receive no First Amendment protection'"); State v. Crawley, 819 N.W.2d 94, 119–20 (Minn. 2012) (noting that federal precedent is binding on the state court and that, "the reasoning of Justice Breyer's concurring opinion makes clear that knowing falsehoods are entitled to First Amendment protection . . . Indeed, the concurrence explained that the Court's prior statements on the lesser First Amendment value of false statements could not be read to 'mean no protection at all.'").

[56] *See, e.g.,* Richard Hasen, *A Constitutional Right to Lie in Campaigns and*

The Court indicated lies might be unprotected when they cause some other "legally cognizable harm."[57] Rebecca Green argues there is narrow agreement some kind of harm – albeit one subject to further refinement – must emerge from a lie for it to be unprotected. Here, I explicate these harms as imagined by legislators and the laws they pass.[58]

However, this approach to interpreting *Alvarez* is not universal. Rather than focusing on specific statements in the ruling, Chen and Marceau examine the opinions wholistically, arguing neither opinion is "narrower" than the other because each "invokes different, and incompatible, tiers of scrutiny."[59] They write, "although the [plurality and concurrence] . . . agreed that the First Amendment protects the lies in question, there is no shared reasoning or commonality of approach as to the applicable level of scrutiny. Neither opinion is 'narrower,' nor is there any 'shared agreement[.]'"[60] This is indicative of their proposition that the difference in the case is one of kind, not one of degree.[61]

However, the Ninth Circuit challenged their argument that these are "incompatible[] tiers of scrutiny." The Circuit reconciled *Alvarez* by saying, at minimum the plurality and concurrence require meeting intermediate scrutiny, and the relevant case did not meet intermediate scrutiny.[62]

Chen and Marceau also suggest that, when confronted with cases involving lying, courts have begun leaning towards strict scrutiny "when the lies targeted by government action are of a 'political' nature."[63] Since deepfakes of political candidates or ones that attempt to influence voting behavior are of a "political nature," this finding supports the argument deepfakes are covered by many of the old laws discussed below.

Elections?, 74 MONT. L. REV. 53, 69 (2013) ("Gone is the argument, accepted by some courts before *Alvarez*, that false speech [including false campaign or election speech] is entitled to no constitutional protection and in a category with obscenity and fighting words."); Alan K. Chen & Justin Marceau, *Developing a Taxonomy of Lies Under the First Amendment*, 89 COLO. L. REV. 656, 656 (2018) ("The decision rejected the government's claim that lies are a form of speech that is categorically outside the scope of the First Amendment's coverage."); *Accord*. Joshua S. Sellers, *Legislating Against Lying in Campaigns and Elections*, 71 OKLA. L. REV. 141, 147–48 (2018).

[57] *Alvarez*, 567 at 71 (plurality opinion).

[58] *See infra* § IV.A.

[59] Chen & Marceau, *supra* note 56, at 673.

[60] *Id.*; *cf*. *Animal Legal Def. Fund*, 264 F. Supp. 3d at 1201–02.

[61] The differences in kind and not of degree reasoning was adopted by the court in *Animal Legal Def. Fund*, 264 F. Supp. 3d. at 1210.

[62] United States v. Swisher, 811 F.3d 299, 317 n.13 (9th Cir. 2016) ("[W]e need not determine whether the plurality opinion or Justice Breyer's opinion constitutes the holding[.]").

[63] Chen & Marceau, *supra* note 56, at 674.

3. Legal Implications of Deepfakes

While Chesney and Citron initiated the legal writings on deepfakes, scholarship on it has grown, and can be classified into three categories: writings about the first amendment implications of deepfakes, assessing if deepfakes violate existing laws, and approaching deepfakes as form of misinformation or disinformation.

First, scholar Marc Blitz's extensive writings on First Amendment implications of deepfakes is highly technical and theoretical, focusing on the distinction between "coverage," "protection," and "authorship."[64] In the political context, some, "narrowly crafted injunctions against defamatory political deepfakes should be permitted."[65] Bryn Wells-Edwards considered audio deepfakes and voice in the political context, focusing on defamation and false light.[66] By exclusively analyzing the specific medium of deepfakes and discussing the availability of injunctive relief, this work prefaces variation among new state laws. Finally, other work is more democracy and First Amendment focused.[67]

Second, several student notes have broadly asked the question "do deepfakes run afoul of an existing law?" They approach this question from perspectives like privacy, defamation, trademark, and copyright law.[68]

Third, legal scholars have examined deepfakes from an

---

[64] *See* Marc Jonathan Blitz, *Deepfakes and Other Non-Testimonial Falsehoods: When Is Belief Manipulation (Not) First Amendment Speech?*, 23 YALE J. L. & TECH. 160 (2020).

[65] Jessica Ice, Note, *Defamatory Political Deepfakes and the First Amendment*, 70 CASE W. RSRV. L. REV. 417, 419 (2019).

[66] *See* Bryn Wells-Edwards, Note, *What's in a Voice? The Legal Implications of Voice Cloning*, 64 ARIZ. L. REV. 1213 (2022).

[67] Matthew Bodi discussed First Amendment questions including, "are deepfakes protected speech?" *See* Matthew Bodi, *The First Amendment Implications of Regulating Political Deepfakes*, 47 RUTGERS COMPUT. & TECH. L. J. 143 (2021). My comparative approach is more thorough than his brief five-paragraph comparison of Texas and California deepfake laws. While his comparative analysis was descriptive and emphasized liability, it did not deeply examine impact. I expand the descriptive analysis and distinguish myself by covering more states, using additional evidence, and focusing my comparison on intent. For other examples, *see* Alyssa Ivancevich, Note, *Deepfake Reckoning: Adapting Modern First Amendment Doctrine to Protect Against the Threat Posed to Democracy*, 49 HASTINGS CONST. L. Q. 61 (2022); Lindsey Wilkerson, Note, *Still Waters Run Deep(fakes): The Rising Concerns of "Deepfake" Technology and Its Influence on Democracy and the First Amendment*, 86 MO. L. REV. 407 (2021).

[68] *See, e.g.*, Philip Boyd, *Fakes and Deepfakes: Balancing Privacy Rights in the Digital Age*, 74 ALA. L. REV. 517 (2022) (privacy); Ice, *supra* note 65 (defamation); Quentin J. Ullrich, Note, *Is This Video Real? The Principal Mischief of Deepfakes and How the Lanham Act Can Address It*, 55 COLUM. J. L. & SOC. PROBS. 1 (2021) (trademark); Wells-Edwards, *supra* note 66 (copyright).

informational perspective, examining the legality of disinformation and fake news in elections and postulating different ways to stop it.[69] Proposals include creating a "right of reply" for deepfakes of digital content and setting up a regulatory body to investigate claims of deepfakes (a type of "truth commission").[70] Either or both would institutionalize a process for responding to deepfakes, lending legitimacy to claims made about deepfakes from the subject of them (i.e. help determine if the Liar's Dividend is being invoked).

4. Legal Scholarship on Deepfakes and Elections

Rick Hasen argues for a new disclosure regime to protect the information ecosystem.[71] His argument supporting their constitutionality follows from the government's interest in regulating false information, and is "surprisingly easy to make" because significant case law emphasizes "democracy depends upon voters' ability to evaluate arguments in order to make political and electoral decisions."[72] He mentions the impact of the intent requirement and differences between verbs in the definitions like "manipulated" and "altered" in deepfake prohibition laws in effect at publication.[73]

Rebecca Green's article considers statements falsely or wrongly purporting to emanate from candidates or campaigns, which she terms "counterfeit campaign speech." She narrowly defines it to only cover content which, "materially alter[s] a candidate's message and pass[es] it off as authentic; it would only reach manipulation of candidate source material."[74] She argues this definition is sufficiently narrow to meet the state's "compelling interest in protecting voters, elections, and

---

[69] *See, e.g.*, RICHARD HASEN, CHEAP SPEECH: HOW DISINFORMATION POISONS OUR POLITICS—AND HOW TO CURE IT (2022); Overton, *supra* note 28; Marshall, *supra* note 28; David O. Klein & Joshua R. Wueller, *Fake News: A Legal Perspective*, 20 J. INTERNET L. (2017).

[70] *See* Elizabeth F. Judge & Amir M. Korhani, *A Moderate Proposal for a Digital Right of Reply for Election-Related Digital Replicas: Deepfakes, Disinformation, and Elections*, *in* CYBER-THREATS TO CANADIAN DEMOCRACY (Holly Ann Garnett & Michael Pal eds., 2022), https://papers.ssrn.com/abstract=3827249 (proposing a right of reply); Richard Painter, *Deepfake 2024: Will Citizens United and Artificial Intelligence Together Destroy Representative Democracy?*, 14 J. NAT'L SEC. L. & POL'Y 121 (2023) (proposing a regulatory body); Hasen, *supra* note 56, at 75–76 (arguing a government "truth commission" is likely constitutional).

[71] *See* Richard Hasen, *Deep Fakes, Bots, and Siloed Justices: American Election Law in a Post-Truth World*, 64 ST. LOUIS U. L. J. 535 (2020).

[72] *Id.* at 545.

[73] *See id.* at 552–553.

[74] Rebecca Green, *Counterfeit Campaign Speech*, 70 HASTINGS L. J. 1145, 1453 (2019).

candidates from faked election speech."[75]

Our work is complementary, and we agree existing laws are insufficient.[76] We both examine specific statutes and ask if they can be used to prohibit deepfakes. Her analysis of "highly-specific bans" of specific types of speech is shorter than mine.[77] She emphasizes laws prohibiting misrepresenting public officials, using misleading caller information, and committing identity theft, while I examine voter intimidation, civil rights, and anti-conspiracy laws.[78]

II. METHODS

This Part contextualizes and justifies my methodology, including inclusion/exclusion criteria, data gathering process, transcription, coding, and analytical methods. Additionally, it reviews methodology for finding old laws.

I endeavor to describe my methodology because the use of interdisciplinary methods is consistent with law and qualitative research. Qualitative data methods like transcription, coding, and thematic analysis were applied to legal texts to understand risks envisioned by the speakers and authors. These methods were used to assist in building legal theory to answer the research questions. These methods help excavate decision making processes, making them consistent with qualitative research and my research questions.[79] Other legal scholars may wish to replicate steps to assist with state level work or work using committee hearing.

A. On Qualitative (Legal) Methods

The literature on legal research methodology is sparse; where it exists, its methodological language differs from the social sciences. "Qualitative legal research" is defined in opposition to quantitative legal research.[80] Qualitative work analyzes texts, seeks patterns and trends,

---

[75] *Id.* at 1449.
[76] *See id.* at 1471 ("Most state election codes, however, do not feature applicable affirmative prohibitions.").
[77] *Id.* at 1470.
[78] *See id.*
[79] *See* Nikolitsa Grigoropoulou & Mario L. Small, Comment, *The Data Revolution in Social Science Needs Qualitative Research*, 6 NATURE HUM. BEHAV. 904 (2022).
[80] Ian Dobinson & Francis Johns, *Legal Research as Qualitative Research*, *in* RESEARCH METHODS FOR LAW 18, 19 (Mike McConville & Wing Hong Chui eds., 2 ed. 2017) ("Qualitative legal research [is] define[d] as simply non-numerical and as such, contrasted with quantitative (numerical) research.").

and crafts arguments based on them.[81] Unlike social science research, legal scholarship is less concerned about data quality, positionality, and inclusion/exclusion criteria. Even when legal scholars conduct case studies, they approach evidence considered by courts *a priori* and do not investigate the role of the Rules of Evidence in shaping the legal reasoning and outcome; legal scholars examine evidence in a vacuum.[82]

Thus, qualitative and legal scholars speak different languages, even though they use similar methods like case studies.[83] Katerina Linos and Melissa Carlson's attempt to bridge this gap is insightful.[84] They argue doctrinal work lacks generalizability and has selection bias by virtue of selecting cases from precedential courts.[85] They suggest that more extensive sampling methods are needed to make generalizable claims, requiring consideration of counterfactuals.[86] Counterfactuals can come from alternative arguments presented in briefs and in dissenting and concurring opinions.[87] However, their focus on rigorous sampling methods misunderstands the point of qualitative research, which is to theory build and not to make generalizable findings.[88]

---

[81] *See, e.g.*, Abbe R Gluck, *The States as Laboratories of Statutory Interpretation: Methodological Consensus and the New Modified Textualism*, 119 YALE L. J. 1750 (2010) (classifying state statutory interpretation schemes based on a reading of case law); Richard L. Hasen, *Reining in the Purcell Principle*, 43 FLA. ST. U. L. REV. 427 (2016) (identifying an emergent legal principle based a close reading of case law).

[82] This is increasingly concerning because recent scholars have focused on the importance (and problems) of using the entire docket, rather than just published opinions, in legal research. *See, e.g.*, Zachary D. Clopton & Aziz Z. Huq, *The Necessary and Proper Stewardship of Judicial Data*, 76 STAN. L. REV. 893 (2024) (discussing how docket and judicial data are recorded and lost when being uploaded to docket searches and commercial legal search engines).

[83] *See, e.g.,* Lisa L. Miller, *The Use of Case Studies in Law and Social Science Research*, 14 ANN. REV. L. & SOC. SCI. 381 (2018).

[84] Katerina Linos & Melissa Carlson, *Qualitative Methods for Law Review Writing*, 84 U. CHI. L. REV. 213 (2017).

[85] See *id.* at 217 ("Many doctrinal research projects suffer from selection bias . . . [s]ampling methods are particularly helpful for these projects and allow legal scholars to generalize beyond the specific cases they analyze in depth.").

[86] *See id.* at 218 ("When, however, scholars wish to generalize these descriptive claims to a broader population of cases, sampling techniques are needed. And all causal claims require careful thinking about counterfactuals.").

[87] *See id.* at 219 ("The adversarial process inherently offers (at least) two alternative ways of understanding a set of facts–the plaintiffs and the defendant's. Amicus briefs and other third-party interventions can also help sketch out alternative options. Additionally, separate opinions from judges, including powerful concurrences and dissents, provide a range of plausible alternative legal outcomes. Furthermore, trial and appellate court judges can offer different answers to the same question, creating legally plausible alternative conclusions.").

[88] For a review of the importance of theory in qualitative research, *see, e.g.,*

B. Selection and Data Collection

The unit of analysis analyzed is laws which have been passed and enacted at the state level prior to 30 April 2024.[89] 14 met this criterion. I identified laws using Public Citizen's deepfake legislation tracker, which was updated throughout the 2024 Legislative session.[90]

To acquire committee hearings and documentation, each state's bill tracker was accessed, requiring navigating a different user interface. Full text of the engrossed (final) version of the bill was downloaded. State legislative materials are notoriously decentralized; to reduce search costs emails were sent to each state's legislative library and/or research team asking to be pointed to recordings of committee hearings on the bill. With their assistance, 42 hearings in 14 states were identified.

The extreme decentralization in materials is a major reason there is little legal scholarship on the state level; federal materials are significantly more centralized. For example, no state library/research teams had the same name, and no states had the same user interface. A tracking spreadsheet organized this information and logged responses.

Another spreadsheet was made with the 42 hearings and metadata about them, including the state, date, committee, and hearing URL. During transcription, the length of the portion of the hearing devoted to the bill, the length of the total hearing, and the method used to transcribe the hearing were added.

Two exclusion criteria removed two states each. First, courts prefer committee hearings over floor hearings when looking for intent because they have more subject matter expertise and are less political.[91]

Christopher S. Collins & Carrie M. Stockton, *The Central Role of Theory in Qualitative Research*, 17 INT'L J. QUALITATIVE METHODS 1 (2018); Kathleen M. Eisenhardt et al., *Grand Challenges and Inductive Methods: Rigor without Rigor Mortis*, 59 ACAD. MGMT. J. 1113 (2016).

[89] *See* Linos & Carlson, *supra* note 84, at 222 ("By defining the limits of their sample, the authors strengthen the plausibility of their inferences.").

[90] *Tracker: State Legislation on Deepfakes in Elections*, PUBLIC CITIZEN (2023), https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/ (last visited July 20, 2024).

[91] *See* Zuber v. Allen, 396 U.S. 168, 186 (1969) ("A committee report represents the considered and collective understanding of those Congressmen involved in drafting and studying proposed legislation. Floor debates reflect, at best, the understanding of individual Congressmen. It would take extensive and thoughtful debate to detract from the plain thrust of a committee report in this instance."); Schwegmann Bros. v. Calvert Distillers Corp., 341 U.S. 384, 395–96 (1951) (Jackson, J., concurring) ("I think we should not go beyond Committee reports, which presumably are well

The research questions ask about legislative intent, necessitating this criterion. This completely excluded New York and Mississippi (they only had recordings from the chamber floor), along with five hearings in California and Wisconsin. Second, the investigation revealed New Mexico and Oregon's websites could not be accessed from outside the United States, so they were excluded because materials could not be accessed. This resulted in a final dataset of 25 hearings on 10 state bills.[92]

Depending on the availability of automatic transcription tools from state legislatures, hearings were either transcribed manually, transcribed automatically through manual verification, or transcribed through Microsoft Word with manual verification. Details of each of the 25 hearings, including its transcription method, are in Appendix 2.

C. Coding and Analysis

Transcripts were imported into NVivo for two rounds of inductive coding, proceeding alphabetically by state. Coding was guided by the research question, so codes were only applied to substantive portions of the transcripts (i.e. not to legislative procedure).

The first round coded high-level risks and concerns about potential deepfake harms. The persuasive act of describing the bill to colleagues allowed the sponsor to articulate their envisioned risks. Other codes focused on alternative solutions to deepfakes and legal concerns raised by the bill. These revealed themselves in statements of non-sponsoring legislators.

Between rounds a coding hierarchy was ideated to make sense of the dispersed codes and organize risks.[93]

The second round deconstructed the different risk models in more

---

considered and carefully prepared . . . [T]o select casual statements from floor debates, not always distinguished for candor or accuracy, as a basis for making up our minds what law Congress intended to enact is to substitute ourselves for the Congress in one of its important functions."). *See generally* VALERIE C. BRANNON, CONG. RSCH. SERV., R45153, STATUTORY INTERPRETATION: THEORIES, TOOLS, AND TRENDS (2023).

[92] For the bills, *see* Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019); H.B. 919, 126th Leg., Reg. Sess. (Fla. 2024); H.B. 664, 68th Leg., Reg. Sess. (Idaho 2024); H.B. 1133, 123rd Gen. Assemb., Reg. Sess. (Ind. 2024); H.B. 5144, 102nd Leg., Reg. Sess. (Mich. 2023); H.F. 1370, 93rd Leg., Reg. Sess. (Minn. 2023); S.B. 751, 86th Leg., Reg. Sess. (Tex. 2019); S.B. 131, 65th Leg., Gen. Sess. (Utah 2024); S.B. 5152, 68th Leg., Reg. Sess. (Wash. 2023); Assemb. B. 664, 2023-2024 Leg., Reg. Sess. (Wis. 2024); *see also* Appendix 1 providing a conversion between each bill and the location in state code it is enacted as statute.

[93] *See* Tom Richards & Lyn Richards, *Using Hierarchical Categories in Qualitative Data Analysis*, *in* COMPUTER-AIDED QUALITATIVE DATA ANALYSIS: THEORY, METHODS AND PRACTICE 80 (Udo Kelle et al. eds., 1995) (arguing code hierarchies are a useful tool in organizing codes and making sense of otherwise disparate codes).

depth, emphasizing how a specific action or fact was a risk. For example, the "election year" code was created in the second round, as it operationalized a specific type of "election security" risk. This revealed itself between rounds.

After the second round, a coding hierarchy was created based on four potential themes. A theory diagram was created linking them together.

Informed by the theory diagram, claim tables were made presenting potential themes and their subcomponents. They contained the state, speaker, hearing, quote, rudimentary analysis, sub-claim it represented, and the strength of the quote. This last aspect adopts Rockmann and Vough's framework of partial, tantalizing, workhorse, and anchor quotes.[94] This process indicated only three were viable (supported by sufficient evidence). The three themes indicated different risks and claim tables focused on identifying their subcomponents.

D. Old Laws

Shifting to RQ2, preexisting laws were identified based on well-known provisions of election law, including causes of action used in civil litigation over the last five years. This was supplemented with relevant criminal provisions listed in the Department of Justice's Prosecution Guide for Election Crimes.[95] The laws discussed in § 3.1.2 and § 3.4.2 drew on Ardia and Ringel who summarized and categorized over 150 state laws.[96] Their footnotes were searched for the 10 states of interest, revealing 37 laws which were recorded in a spreadsheet. Each law's text was briefly reviewed to assess its potential usefulness and brief notes were written.

Case law was examined using Westlaw's "Citing References" feature. For example, some California laws were cited in 12 cases,[97] while

---

[94] *See* Kevin W. Rockmann & Heather C. Vough, *Using Quotes to Present Claims: Practices for the Writing Stages of Qualitative Research*, ORG. RSCH. METHODS, 9–10 (2023).

[95] U.S. Dep't of Just., PROSECUTION GUIDE FOR ELECTION CRIMES, 33–79 (8th ed. 2017) (statutes related to Corruption of the Election Process).

[96] *See* David S. Ardia & Evan Ringel, *First Amendment Limits on State Laws Targeting Election Misinformation*, 20 FIRST AMEND. L. REV. 291 (2022).

[97] As an illustrative example, California had two laws dealing with voter intimidation, *see* CAL. ELEC. CODE § 18502 (West 2024); CAL. ELEC. CODE § 18540 (West 2024). § 18502 proved to be less useful and was cited by four cases. *See* United States v. Tan Duc Nguyen, 673 F.3d 1259 (9th Cir. 2012); United States v. Tan Duc Nguyen, No.

one Florida law was cited in 21 cases.[98] All cases were read for relevance. A separate document was created containing a running list of thoughts on different cases, quotations about risk, notes, and analysis about how the law could be used. This helped identify risk models and create a theoretical framework regarding the application of old state laws.

Finally, several sources were consulted for data triangulation.[99] The sponsors of the Wisconsin law testified to their belief § 12.05 could be used to prohibit the fraudulent misrepresentations of candidates.[100] Over email, library staff provided legislative drafting files for changes to § 12.05 in 1973 and 1993, but these did not prove useful.[101] Other sources consulted included California drafting files and recordings of the 1987 hearings on Texas' § 255.004, originally passed in 1987 (obtained through public records request). Federal Election Commission Matters Under Review were searched and analyzed to identify risk models and limitations.[102]

SACR 08-251 DOC, 2010 WL 374967 (C.D. Cal. Jan. 25, 2010), *aff'd*, 673 F.3d 1259 (9th Cir. 2012); People v. Lee, 107 Cal. 477 (1895); Lincoln v. Lopez, 77 Cal. App. 5th 922 (2022). In contrast, § 18540 was cited in eight cases. *See* United States v. Tan Duc Nguyen, 673 F.3d 1259 (9th Cir. 2012); Koller v. Harris, 312 F. Supp. 3d 814 (N.D. Cal. 2018); United States v. Tan Duc Nguyen, No. SACR 08-251 DOC, 2010 WL 374967 (C.D. Cal. Jan. 25, 2010), *aff'd*, 673 F.3d 1259 (9th Cir. 2012); DeMille v. Am. Fed'n of Radio Artists, 31 Cal. 2d 139 (1947); Citizens for Clean Water v. Reg'l Water Quality Control Bd., No. 2D CIVIL B231945, 2012 WL 5265951 (Cal. Ct. App. Oct. 25, 2012) (unpublished opinion); Hardeman v. Thomas, 208 Cal. App. 3d 153 (Ct. App. 1989); Stebbins v. White, 190 Cal. App. 3d 769 (Ct. App. 1987); Miller v. Childs, 28 Cal. App. 478 (Cal. Ct. App. 1915).

[98] Florida has two voter intimidation laws. *See* FLA. STAT. ANN. § 104.0515 (West 2024) (4 citations); FLA. STAT. ANN. § 104.061 (West 2024) (17 citations). Four proved exceptionally useful in fleshing out risk models. *See* Trushin v. State, 425 So. 2d 1126 (Fla. 1982) (citing § 104.061); Russ v. State, 832 So. 2d 901 (Fla. Dist. Ct. App. 2002) (citing § 104.061 and § 104.0515); State v. Brown, 298 So. 2d 487 (Fla. Dist. Ct. App. 1974) (citing § 104.061); Shiver v. Apalachee Pub. Co., 425 So. 2d 1173 (Fla. Dist. Ct. App. 1983) (citing § 104.061).

[99] *See* Lorelli S. Nowell et al., *Thematic Analysis: Striving to Meet the Trustworthiness Criteria*, 16 INT'L J. QUALITATIVE METHODS 1, 5 (2017) ("Qualitative researchers may triangulate different data collection modes to increase the probability that the research findings and interpretations will be found credible.").

[100] *Hearing on Assemb. B. 664 Before the Assemb. Comm. on Campaigns & Elections*, 2023-2024 Reg. Sess. (Wis. 2024) (Jan. 9, 2024) (statement of Rep. Jimmy Anderson). *See generally* WIS. STAT. ANN. § 12.05 (West 2024).

[101] The law originated in 1911, but this drafting file is over 1000 pages and only available on microfilm and therefore could not be scanned. *See* Email from Bryce Grunwaldt, Research Assistant at the Wisconsin Legislative Reference Bureau, to Candidate 1083032 (June 10, 2024) (on file with author).

[102] *See generally* FED. ELECTION COMM'N, GUIDEBOOK FOR COMPLAINTS AND RESPONDENTS OF THE FEC ENFORCEMENT PROCESS (May 2012); FED. ELECTION COMM'N,

III. RQ3: ANALYZING OLD LAWS

There are five categories of risks old election laws are set up to deal with and which could be used to prohibit deepfakes: voter intimidation, conspiracies against rights, robocalls, fraudulent misrepresentations, and impeding others from giving their support or advocacy to candidates. This Part concludes by bringing these risks together to sketch the model responsive to RQ3; case law indicates deepfakes must have certain properties or characteristics to be covered under these laws, meaning the laws are not generally applicable to all political deepfakes.

A. Risk 1: Voter Intimidation

State and federal laws prohibiting voter intimidation could be useful if deepfakes intimidate voters. However, the fact that states have their own laws indicates that state and federal laws might be concerned with different risks. Therefore, I examine these separately by conducting a close reading of the laws and case law to theorize different risk models.

Two cases involving the same facts have been targeted by federal and Michigan laws, making it an insightful case study. These are *Wohl* (federal civil case) and *Burkman* (Michigan criminal case). In brief, Jacob Wohl and Jack Burkman sent approximately 85,000 robocalls to phone numbers associated with predominantly black cities (like Philadelphia and Detroit) which stated voting by mail would lead to their information being published for police to use to track down old warrants, by debt collectors to find outstanding debts, and by the Center for Disease Control to track down people who were not vaccinated.[103]

1. Federal Prohibition

Section 11(b) of the Voting Rights Act prohibits (attempting to) intimidate voters.[104] Importantly, it intentionally lacks a requirement for

---

FEC Enforcement Query System, https://www.fec.gov/data/legal/search/enforcement/ (last visited July 26, 2024). For an example of how these can be used as primary evidence, *see* Matthew S. Raymer, *Fraudulent Political Fundraising in the Age of Super PACs*, 66 SYRACUSE L. REV. 240 (2016).

[103] *See* Nat'l Coal. on Black Civic Participation v. Wohl, 661 F. Supp. 3d 78, 91–95 (S.D.N.Y. 2023) (*Wohl II*) (discussing the factual background of the case).

[104] *See* Voting Rights Act of 1965 § 11(b), 52 U.S.C.A. § 10307 ("No person, whether acting under color of law or otherwise, shall intimidate, threaten, or coerce, or attempt

the actor to intend for their acts to be intimidating. According to the bill s drafter, Attorney General Nicholas Katzenbach, prior intimidation laws had more onerous requirements, limiting their usefulness.[105] The law, he testified,

> represents a substantial improvement over [a precursor law], which now prohibits voting intimidation. Under [section 11(b)] no subjective purpose need be shown, in either civil or criminal proceedings, in order to prove intimidation under the proposed bill. Rather, defendants would be deemed to intend the natural consequences of their acts. This variance from . . . [the earlier law] is intended to avoid the imposition on the Government of the very onerous burden of proof of purpose which some district courts have – wrongfully, I believe – required.[106]

Moreover, 11(b) covers individual actions from the time after voter registration, so voters who see an intimidating deepfake and are registered would be covered.[107] Federal courts have expanded the meaning of intimidate," to include physical,[108] economic,[109] or coercive

---

to intimidate, threaten, or coerce any person for voting or attempting to vote, or intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person for urging or aiding any person to vote or attempt to vote, or intimidate, threaten, or coerce any person for exercising any powers or duties under [certain other provisions] of this title.").

[105] These laws were § 131(b) of the Civil Rights Act of 1957 and § 2 of the Enforcement Act of 1871. On their limitations, *see* Ben Cady & Tom Glazer, *Voters Strike Back: Litigating against Modern Voter Intimidation*, 39 N.Y.U. REV. L. & SOC. CHANGE 173, 193 (2015) ("Unlike section 131[b], which requires that plaintiffs prove racial motivation, or the KKK Act, which requires a conspiracy among the defendants, all a section 11[b] claim requires is a nexus between the defendant's conduct and a voting related activity and a showing that the defendant's conduct was objectively intimidating, threatening, or coercive.").

[106] *Hearing on the Voting Rights Act of 1965 Before the H. Comm. on the Judiciary*, 89th Cong. 12 (1965) (statement of Att'y Gen. Nicholas deB. Katzenbach).

[107] In response to a hypothetical about the time where Section 11(b) can be used, *see id.* ("No, he has gotten registered already under the assumption of section 7. So I would think the intimidation, threatening, or coercing would apply to any period of time after that registration up through the when he could have voted.")

[108] *See* United States v. Wood, 295 F.2d 772 (5th Cir. 1961) (courthouse official physically beat a Black voter registration volunteer in front of black residents trying to register); United States v. Original Knights of the Ku Klux Klan, 250 F. Supp. 330 (E.D. La. 1965) (pattern of violence against black citizens in Washington Parish, Louisiana).

[109] *See* United States v. Bruce, 353 F.2d 474 (5th Cir. 1965) (white landowners ordered Black businessman who assisted in registering voters to stay off their property, preventing him from reaching his clients).

threats[110] taking place at sites like voting booths, voter registration meetings, or when filling out absentee ballots.[111]

Wohl was a civil case alleging violations of voter intimidation laws like §11(b).[112] The State of New York intervened to protect all New York voter s rights and alleged state election law violations.[113] The case settled before trial.[114]

The bulk of the original judicial analysis came at the temporary restraining order stage because injunctive relief requires an early assessment of the likelihood of success of the merits of a case.[115] In the order, Judge Marrero required the defendant to call voters back to inform them they were victims of deception.[116] The order acknowledged the difficulty in fully remedying harms to voting; the second call tried to return voters to square one" before the phone call.[117] This demonstrates the limits of injunctive relief: it only prohibits further spreading and does not provide a remedy for the people who have already been exposed to deceptive content.

This history of § 11(b) supports the argument that the law can be used to recover damages for people who are intimidated by deepfakes. The law's focus on effects makes it more plaintiff friendly, emphasizing interpretation by voters, not intent of the creator. The broad extension of

---

[110] *See* Paynes v. Lee, 377 F.2d 61 (5th Cir. 1967) (white citizens threatened to "destroy" and "annihilate" a Black man who tried to register to vote); *Original Knights of the Ku Klux Klan*, 250 F. Supp. 330 (pattern of violence against Black citizens in Washington Parish, Louisiana).

[111] *See* Cady & Glazer, *supra* note 105, at 195 n.139 (collecting cases).

[112] *See* Complaint, Nat'l Coal. on Black Civic Participation v. Wohl, No. 1:20-cv-08668 (S.D.N.Y. Oct. 19, 2020), ECF No. 11.

[113] *See* Complaint in Intervention, Nat'l Coal. on Black Civic Participation v. Wohl, No. 1:20-cv-08668 (S.D.N.Y. May 19, 2021), ECF No. 102.

[114] *See* Proposed Consent Decree, Nat'l Coal. on Black Civic Participation v. Wohl, No. 1:20-cv-08668 (S.D.N.Y. April 8, 2024), ECF No. 343.

[115] *See* Winter v. Nat. Res. Def. Council, Inc., 555 U.S. 7 (2008).

[116] *See* Nat'l Coal. on Black Civic Participation v. Wohl, 498 F. Supp. 3d 457, 489–90 (2020) (*Wohl I*) ("[I]t is hereby . . . ordered that Defendants shall send, or authorize an appropriate third party to send, a robocall message [the 'Curative Message'] informing the recipients of the original robocall message discussed in this Decision and Order [the 'Prior Robocall'] of this Court's findings regarding that call. The Curative Message shall be issued to all recipients of the Prior Robocall and shall state only the following [predetermined message].").

[117] *See id*. at 489 ("[R]estraining Defendants from engaging in further unlawful conduct would not suffice to undo the harm they have brought about in this case. In order to mitigate the damage Defendants have caused and thus endeavor to return the robocall recipients to the position they were in before Defendants placed those calls, the Court considers it necessary for Defendants to issue a message to all recipients of the robocalls informing them about this Court's finding that Defendants' original message contained false statements that have had the effect of intimidating voters, and thus interfering with the upcoming presidential election, in violation of federal voting-rights laws.").

threats covered means deepfakes depicting a variety of situations should be covered. For example, a deepfake depicting violence to individuals who vote a certain way, or that falsely depicts people with lost jobs. It should also cover deepfakes depicting or insinuating violence against individuals running voter registration drives. Finally, if someone made a deepfake of people claiming to be from Springfield, Ohio eating pets and used the video as false evidence, and this video led to threats intimidating the depicted individual(s), this situation may be covered.[118] Despite these examples, § 11(b)'s usefulness is constrained by the fact that it only applies to intimidation, and not mere "misrepresentation" which is not covered.

2. State Prohibition

While the federal government treats voter intimidation as a civil matter, states treat it as a criminal offense.[119] They differ regarding how they treat intent, with 29 only imposing liability if the speaker intended to intimidate while 17 apply it to the actual effect of the conduct.[120] This is representative of the variation found in these laws and their interpretation. *Burkman* is a good comparison case because it allows us to compare the differences in risks between federal and state laws when the same conduct is at issue.

Burkman is a Michigan criminal case alleging this conduct violated a state law prohibiting voter intimidation. [121] On appeal, Michigan's Supreme Court narrowed the interpretation of "other corrupt means or device" to strictly apply to content concerning "voting

---

[118] This hypothetical draws on a September 2024 conspiracy theory involving President Donald Trump and Springfield, Ohio which has resulted in a growing number of threats. *See* Michael Rubinkam & Julie Carr Smyth, *What to Know about the Threats in Springfield, Ohio, after False Claims about Haitian Immigrants*, AP NEWS (Sep. 22, 2024), https://apnews.com/article/springfield-ohio-haitian-immigrants-threats-key-details-7594bae869fb05dc6f106098409418cc.

[119] For a review of all of the laws and their differences, *see* Ardia & Ringel, *supra* note 96, at 362–66. Voter intimidation laws for the states studied in this article include IND. CODE § 3-14-3-21.5 (West 2024); WASH. REV. CODE ANN. § 29A.84.630 (West 2024); CAL. ELEC. CODE § 18540 (West 2021); UTAH CODE ANN. § 20A-3a-502 (West 2024).

[120] Ardia and Ringel, *supra* note 96, at 365.

[121] *See* MICH. COMP. LAWS ANN. § 168.932(a) (West 2024) ("A person shall not attempt, by means of bribery, menace, or other corrupt means or device, either directly or indirectly, to influence an elector in giving his or her vote, or to deter the elector from, or interrupt the elector in giving his or her vote at any election held in this state.").

requirements and procedures"[122] because prohibiting this conduct has been approved by the Supreme Court.[123]

Several aspects of this decision stand out regarding threats and how the law applies to deepfakes. By default, speech is protected unless it meets a limited number of exemptions, including being a "true threat" to the listener. The Court ruled Burkman's speech did not meet this exemption because the purported threatening actor (e.g. the police) were not under the control of the caller (Wohl and Burkman). The Court ruled a necessary, but not sufficient, condition to being a true threat is if the actor who would carry out the threat is under the control of the speaker.[124] In other words, the Court ruled that an alleged threat cannot be threatening if the speaker has no way of executing the threat as described.

This is problematic. Most threatening messages involve a third party and rely on the recipient not knowing the third party is not under the speaker's control. These messages are now exempt. This could begin a change in the "true threats" exemption because intimidating messages — as long as the intimidation is threatened with a third party — are not subject to this exemption. Therefore, references to police, mafia, or similar actors in deepfakes might increase.

Additionally, the Court's limiting construction of "other corrupt means or device" language indicates the risks the law can address. After exhaustively defining "corrupt" and "means or device" the combined definition they used was "any other depraved or immoral method or scheme of deterring or preventing someone from voting or influencing or interrupting someone in giving their vote."[125] The definition adopts a technology agnostic approach, emphasizing how speech is interpreted

---

[122] *See* People v. Burkman, 15 N.W. 3d 216, 229 (Mich. 2024) ("Specifically, we hold that when the charged conduct is solely speech and does not fall under any exceptions to constitutional free-speech protections, MCL 168.932(a)'s catchall phrase operates to proscribe that speech only if it is intentionally false speech that is related to voting requirements or procedures and is made in an attempt to deter or influence an elector's vote.").

[123] *See id.* (citing Minnesota Voters Alliance v Mansky, 585 U.S. 1, 19 n.4 (2018) ("We do not doubt that the State may prohibit messages intended to mislead voters about voting requirements and procedures.")).

[124] *See id.* at 235. ("[A] legally cognizable threat requires that the speaker, or someone within the speaker's control, be the person who executes the threat. And here, the robocall stated that other third-party actors—police departments, credit card companies, and the CDC—would or likely would be performing the malevolent actions in question without any influence from or control by the purported speaker. Accordingly, we affirm the Court of Appeals' conclusion that defendants' conduct is not excluded from constitutional free-speech protections under the true-threat exception.") (internal citations omitted).

[125] *Id.* at 231.

and aligns to societal values. This indicates a desire to ensure secure elections, making it a societal risk. Central to the definition is how voters interpret the speech and how it is a proximate cause for behavioral change. Therefore, the risks the Court envisions are actions harming voters by deterring, preventing, influencing, or interrupting their vote.

Despite this limitation and its impact on the "true threats" exemption, the law remains broad enough to cover election deepfakes relating to voting procedures which aims to "deter[] . . . or influence[]" voting behavior. Therefore, the risk model centers on adjectives ("deter[] . . . or influence[]"), content (voting procedures), and outcomes (behavioral changes). Thus, deepfakes attempting to dissuade a voter from voting and one saying "save your vote for Wednesday" are covered. The latter spreads false information about a voting procedure. Likewise, a deepfake saying "show your support by not voting" is covered because it undermines the vote-casting and collection process. However, the "and" in the limiting construction means the law does not apply to deepfakes misrepresenting candidates to influence a voter's vote.[126] This limits the law's coverage to false procedural and process information, excluding deepfakes misrepresenting candidates.

B. Risk 2: Conspiracies Against Rights

Next, a civil rights era law can be invoked if deepfakes violate a civil right. 18 U.S.C. § 241 prohibits conspiracies against civil rights and constitutional guarantees,[127] one of which is the right to vote.[128] It can be used in cases where (1) voter intimidation reaches the required, "nexus between the defendant's conduct and a voting-related activity"[129] or (2) if another federally protected right is interfered with. To make full use of this law and test its reach, one consideration should be if the deepfake violates a separate right. For example, the right to association and uncontrolled speech discussed below are a relevant starting place. While

---

[126] *See id.* at 239 ("MCL 168.932(a)'s catchall phrase operates to proscribe that speech only if it . . . is related to voting requirements or procedures *and* is made in an attempt to deter or influence an elector's vote.") (emphasis added).

[127] 18 U.S.C. § 241 ("If two or more persons conspire to injure, oppress, threaten, or intimidate any person in any State, Territory, Commonwealth, Possession, or District in the free exercise or enjoyment of any right or privilege secured to him by the Constitution or laws of the United States, or because of his having so exercised the same . . . They shall be fined under this title or imprisoned not more than ten years, or both.").

[128] *See* 18 U.S.C. § 245 (making the right to vote a federally protected right); Ex parte Yarbrough, 110 U.S. 651 (1884) (holding Congress can punish individuals who violate voting rights in federal elections).

[129] Cady & Glazer, *supra* note 105, at 193.

no judge has yet stated deepfakes violate intellectual property rights, reaching this finding could be a potential avenue to recover damages against individuals and entities making deepfakes.

In *United States v. Mackey*, defendant Douglas Mackey was convicted of violating 18 U.S.C. § 241 for conspiring to deprive individuals of their civil rights by using social media to disseminate false and misleading information about voting procedures during the 2016 presidential election.[130] The alleged purpose was to suppress voter turnout, targeting marginalized communities and swing state voters by posting memes encouraging them to vote from home via text.[131] Approximately 5,600 people attempted to text in their vote.[132] He is currently appealing his March 31, 2023 conviction on multiple grounds, including differing definitions of "injure." Based on case law and statutory history he argues, "[t]o 'deceive' is not to 'injure'."[133] The federal government disagrees[134] while amici Rick Hasen and the Yale Media Center argue impeding the right to vote has been a tortious injury since the early 1700s.[135] Oral arguments for the appeal were heard in April 2024.[136]

Adopting a maximalist view of Mackey's argument "[t]o 'deceive' is not to 'injure'" could have numerous consequences. It means any conspiracy involving deception to violate a federally guaranteed right would not be covered within the Circuit. Many conspiracies, like conspiracy to commit fraud, involve deception, so this could drastically limit the law's scope.[137] Thus, it could represent a radical departure from the federally guaranteed right to vote established in *Ex Parte Yarbrugouh*.[138]

Also, Mackey argues, "'injure' does not naturally cover harms imposed by deception; it typically connotes a coercive act."[139] This

---

[130] *See* Indictment, United States v. Mackey, No. 1:21-cr-00080-AMD, ECF No. 8 (E.D.N.Y. Feb. 10, 2021).
[131] *See* Complaint & Affidavit in Support of an Arrest Warrant, United States v. Mackey, No. 1:21-cr-00080-AMD, ECF No. 1 at 3–4 (E.D.N.Y. Jan. 22, 2021).
[132] *See* Opening Brief of Defendant-Appellant Douglass Mackey at 6, United States v. Mackey, No. 23-7577, Docket No. 44.1 (2d Cir. Jan. 5, 2024).
[133] *See id.* at 19.
[134] *See* Brief for the United States, United States v. Mackey, No. 23-7577, Docket No. 84.1 (2d Cir. Feb. 5, 2024).
[135] *See* Brief for Richard L. Hasen as Amicus Curiae Supporting Appellee and Affirmance at 5–9, United States v. Mackey, No. 23-7577, Docket No. 106.1 (2d Cir. Feb. 12, 2024).
[136] *See* Case Heard, United States v. Mackey, No. 23-7577 (2d Cir. Apr. 5, 2024).
[137] U.S. Dep't of Justice, *supra* note 95, at 20 (collecting cases for how § 241 has been used in election fraud cases).
[138] 110 U.S. 651 (1884).
[139] *See* Opening Brief of Defendant-Appellant Douglass Mackey, *supra* note 132, at 18.

misunderstands "injure" by adopting a strict textualist reading. Rather, "injure" is a term of art describing a legally cognizable harm. Impairment of rights is such a harm. Misdirection and deception can prevent, mislead, or impair the exercise of rights. This barrier is an injury because injuries are a form of harm occurring through a specific overt act. Adopting this reading would prevent the law from being effective against deepfake creators.

C. Risk 3: Robocalls

League of Women Voters of New Hampshire v. Kramer concerns a deepfake Steve Kramer made of President Biden days before the 2024 New Hampshire primary. It told voters to save their vote for November. Kramer's goal was to bring awareness to the risks of deepfakes.[140] The League of Women Voters alleges Kramer violated § 11(b) and New Hampshire laws protecting citizens from unwanted robocalls.[141] The League also alleges the telephone companies (also named as defendants) failed to comply with consumer protection laws.[142] As the first lawsuit about election deepfakes, *Kramer* is a critical test case applying §11(b) to deepfakes. *Wohl* indicates it should be successful due to similar fact patterns.

Kramer indicates three potential paths forward. First, there are already state and federal laws prohibiting robocalls which fail to include certain disclosures and opt-outs. Upon Kramer's calls being reported, the Federal Communication Commission clarified that the law prohibiting "initiat[ing] any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without the prior

---

[140] *See* Alex Seitz-Wald, *A Magician Says a Democratic Operative Paid Him to Make the Fake Biden New Hampshire Robocall That Is under Investigation*, NBC NEWS (Feb. 24, 2024), https://www.nbcnews.com/politics/2024-election/biden-robocall-new-hampshire-strategist-rcna139760; Marcia Kramer, *Steve Kramer Explains Why He Used AI to Impersonate President Biden in New Hampshire*, CBS NEWS (Feb. 26, 2024), https://www.cbsnews.com/newyork/news/steve-kramer-explains-why-he-used-ai-to-impersonate-president-biden-in-new-hampshire/ (Kramer describing his purpose in creating the deepfakes).

[141] *See* First Amended Complaint, League of Women Voters of N.H. v. Kramer, No. 1:24-cv-00073, (D.N.H. May 28, 2024), ECF No. 65.

[142] *See id.* at 2. Paul Carpenter was paid to make the deepfakes but is not named as a defendant. *See also* Seitz-Wald, *supra* note 140. One speculative reason for this could be vicarious liability, the principle that an employer is liable for an employee's conduct, arising under the doctrine of *respondeat superior* (one is responsible for the actions of their subordinates).

express consent of the called party" already applies to deepfakes.[143] Federal law also requires robocalls to identify the origin source and have opt-out mechanisms.[144]

Audio deepfakes are clearly an "[a]rtificial . . . voice", meaning this law already *de-facto* prohibits audio deepfakes being used for mass phone calls. While this interpretation seems obvious, this determination is almost certainly going to be subject to judicial interpretation.[145] Either way, the statute only applies to landlines ("residential telephone lines") which are decreasing in use, meaning the prohibition will apply to a smaller subset of phone calls over time.[146]

Second, the case shows many states have consumer protection laws prohibiting unsolicited phone calls. For example, New Hampshire requires prerecorded political messages to disclose who is paying for the message and prohibits misrepresenting the origin of the call.[147] The legislative history of this law indicates preventing conduct like this was its purpose, strengthening the case the laws should apply to deepfakes.[148]

Third, the case shows that third parties can be held responsible.

---

[143] 47 U.S.C.A. § 227(b)(1)(B) (West 2024); *see* Fed. Commc'n. Comm'n., CG Docket No. 23-362, Declaratory Ruling: in the Matter of Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts (Feb. 8, 2024), https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf.

[144] *See* 47 C.F.R. § 64.1200(b).

[145] *See* Loper Bright Enterprises v. Raimondo, 603 U.S. 369 (2024) (overruling Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984)).

[146] *See* Brett Creech, *Are Most Americans Cutting the Cord on Landlines?*, BEYOND THE NUMBERS (May 20, 2019), https://www.bls.gov/opub/btn/volume-8/are-most-americans-cutting-the-cord-on-landlines.htm (finding declining spending on residential telephone lines between 2007 and 2017); *cf.* Courtney Kennedy, Kyley McGeeney & Scott Keeter, *The Twilight of Landline Interviewing*, PEW RSCH. CTR. (Aug. 1, 2016), https://www.pewresearch.org/methods/2016/08/01/the-twilight-of-landline-interviewing/ (discussing the impact of declining landline usage on surveys); Russell Heimlich, *Polling: The Cell Phone Challenge*, PEW RSCH. CTR. (May 26, 2010), https://www.pewresearch.org/short-reads/2010/05/26/polling-the-cell-phone-challenge/ (same).

[147] N.H. Rev. State. § 664:14-a (source of payment); N.H. Rev. State. § 664:14-b (source of call).

[148] Regarding N.H. Rev. State. § 664:14-a, *see Hearing on H.B. 332, Before the H. Election Law Comm.*, 158th General Court, 2003 Reg. Sess. (N.H. 2003) (statement of Rep. Paul Spiess) ("I have no problem with the practice of a candidate or volunteers taking their time and energy to make a personal call to a registered voter. I have a significant concern with allowing the unregulated use of pre-recorded messages sent out in mass by automatic dialing systems on a repetitive basis to individuals who are unaware who is behind the call."). Regarding N.H. Rev. State. § 664:14-b, *see* N.H. H.REC. JOURNAL, 161st General Court, 2009 Sess., Vol. 31, No. 16, at 5, (Feb. 27, 2009) ("Current law does not prohibit – and therefore implicitly permits – a political campaign to make campaign calls in the name of another, perhaps competing, political campaign. This law resulted in some political campaigns to make deceptive and mean-spirited calls to unsuspecting voters. The committee believes elections should be won by a competition of ideas, not dirty tricks.").

The telephone operators who handled the phone calls and phone lines were named as defendants, and their efforts to be dismissed were unsuccessful. Ultimately, the May 2025 settlement decree required the defendants to create a dedicated compliance team and implement a detailed compliance plan to prevent future transmission of misleading robocalls.[149]

D. Risk 4: Fraudulent Misrepresentations

State and federal laws intend to prevent people from misrepresenting themselves as someone else.

1. Statements About Fundraising

Federal campaign finance law prohibits misrepresenting yourself as another candidate or party when making statements or raising money to mitigate fraud and reduce corruption in politics.[150] However, the efficacy of the fundraising portion of regulations is questionable because it does not apply to all types of political entities like third parties, potentially exempting them from this rule and its use with deepfakes. This law was passed in 2002 but originated earlier, so it could not have anticipated the rise of third-party finance groups that have been enabled by court decisions since.[151] Additionally, the law only concerns fundraising practices, so campaigns could get around it by not asking for money in their ad. While I suggest it would prohibit deepfakes from being used to solicit funds, this characteristic (solicitation) only pertains to a portion of possible campaign ads. Thus, the law can be said to address "integrity in fundraising."

The law's reach is limited to domestic actors, although investigations can reveal the geographic location of actors and potentially clarify the source of the information.[152] For example, it was used to investigate a website fraudulently representing itself as raising money for Hilary Clinton's 2016 campaign, including photos mimicking her website, a seemingly authentic domain name, and campaign's actual mailing address.[153] The website "tried to deceive American voters into

---

[149] Consent Decree, League of Women Voters of N.H. v. Kramer, No. 1:24-cv-00073 (D.N.H. May 23, 2025), ECF 121.
[150] 11 CFR § 110.16.
[151] *See* Richard Briffault, Super PACS, 96 MINN. L. REV. 1544 (2012) (describing the origin of Super PACS).
[152] *See* 11 CFR § 110.16.
[153] *See* Second General Counsel's Report, Person Unknown, MUR 7194 (Fed. Election Comm'n, May 26, 2020), https://www.fec.gov/files/legal/murs/7194/7194_09.pdf.

believing that they could vote for Clinton via the Website rather than at a polling location."[154] However, it was created by people outside the United States, so no further steps could be taken.[155] This demonstrates the law is unfit for systematically addressing foreign election interference.

2. Other Types of Statements

Other state laws prohibit people from falsely representing themselves as an incumbent, from falsely representing themselves as authorized to speak on someone's behalf, and from making unauthorized endorsements.[156] These addresses a specific representational risk – how the covered entity is perceived – at the expense of how the public perceives the speech. This approach focuses on the speaker, not the listener.

The laws also restrict the ability of candidates to represent themselves in a certain way. These are "factual prohibitions". For example, Texas law prohibits representing oneself as an incumbent, but this does not extend to objects associated with an office.[157] This creates leeway where deepfakes could imply, but not outright say, someone is an incumbent. These laws could be worked around by finding all a state's relevant laws and ensuring deepfakes do not include prohibited representation. But if a deepfake does explicitly violate one of these provisions the law could be invoked.

E. Risk 5: Impeding Giving Support or Advocacy to Candidates

The Ku Klux Klan Act of 1871 was passed to enforce civil rights laws. The "support or advocacy clause" in § 1985(3) prohibits conspiracies by two or more people, "by force, intimidation, or threat, [of] any citizen who is lawfully entitled to vote, from giving his support or advocacy in a legal manner, toward or in favor of the election of any lawfully qualified person." [158] Recently, scholars have addressed questions regarding its unique structure and judicial confusion over

---

[154] *Id.* at 19.
[155] *See id.* at 18–19.
[156] Ardia & Ringel, *supra* note 96, at 350–355, 359–361.
[157] TEX. ELEC. CODE ANN. § 255.006 (West); Ethics Advisory Op. No. 548 (Tex. Ethics Comm'n, Dec. 14, 2018), 2018 WL 11390972 ("In this instance, wearing judicial robes or using a reference to the associate judge as 'Associate Judge, 1000th District Court, Texas County' does not, by itself, represent that the judge holds an office the judge does not hold, and therefore would not violate section 255.006 of the Election Code.")
[158] 42 U.S.C. § 1985(3).

separate clauses of 1985(c),[159] and the nature of the right of action the clause grants.[160]

District Courts have begun developing a test for clause. In *Wohl*, the District Court stated, "[t]he Support or Advocacy Clause requires only that the target of the conspiracy be 'an individual legally entitled to vote who is engaging in lawful activity related to voting in federal elections.'"[161] This is based on the three prong test established at the injunction stage, consisting of, "(1) a conspiracy; (2) the purpose of which is to force, intimidate, or threaten; (3) an individual legally entitled to vote who is engaging in lawful activity related to voting in federal elections."[162] The test focuses on the intimidation aspect of the Support or Advocacy clause. The lack of consideration of "support or advocacy" in this test makes it inadequate (and potentially reduces its application to just voter intimidation and not supporting or advocating for candidates). This is concerning because courts are beginning to adopt it.[163]

However, I am primarily interested in the scope of the phrase "support or advocacy" to determine if it could be utilized to prohibit some deepfakes. Courts have described the clause's goal as establishing "the right to *support* candidates in federal elections."[164] The law's legislative history is complex, and the clause originated as an amendment to a precursor law. [165] This amendment was only discussed briefly and discussion does not indicate the scope of "support or advocacy."[166]

Such an investigation is consistent with precedent, as the Supreme Court, "emphasized the breadth of §§ 241 and 242, and the prosecutorial force that Congress intended."[167] The only case thoroughly investigating the breadth of this clause found it covered both the right to vote and other

---

[159] *See, e.g.,* Note, *The Support or Advocacy Clause of § 1985(3)*, 133 HARV. L. REV. 1382 (2020).
[160] *See, e.g.,* Richard Primus & Cameron O. Kistler, *The Support-or-Advocacy Clauses*, 89 FORDHAM L. REV. 145 (2020) (discussing the history of the clause and its earlier forms).
[161] *Wohl II*, 661 F. Supp. 3d at 110.
[162] *Wohl I*, 498 F. Supp. 3d at 487.
[163] *See, e.g.,* Andrews v. D'Souza, 696 F.Supp. 3d 1332, 1346 (N.D. Ga. 2023) ("[T]he court applies the *Wohl* standard here.").
[164] Kush v. Rutledge, 460 U.S. 719, 724 (1983) (emphasis added).
[165] *See* Primus & Kistler, *supra* note 160, at 151–167.
[166] See CONG. GLOBE, 42d Cong., 1st Sess. 704 (1871). Reprinted at Note, *supra* note 159 at 1391.
[167] United States v. Crochiere, 129 F.3d 233, 238–39 (1st Cir. 1997) (Supreme Court precedent "provides strong support for the proposition that the Reconstruction Era Congress did not intend Section 241 to have a narrow scope.").

methods of giving support or advocacy.[168] In other cases, it has been used to target conspiracies attempting to deceive voters about *who* is on the ballot, which deepfakes could do by creating false association between candidates or by making robocalls with lies in them.[169] Voters have a federal right, "to express their choice of candidate and to have their expressions of choice given full value and effect" and deepfakes injure the "full value" by confusing voters and the information environment.[170] Finally, the law has provided relief when the right to vote has been infringed upon in a non-threatening manner, such as stuffing, manipulating, or omitting ballots.[171]

Accordingly, I make the following tentative hypotheses. Political deepfakes are a "lawful activity related to voting" because lies protected under *Alvarez*. The extent to which deepfakes are covered under this statute – and would *not* be prohibited – is contingent on the scope of "support or advocacy". I hypothesize that they are a form of support or advocacy, indicating a potential tension between this law and new state laws.

F. RQ3 Risk Model

In summary, the risk model developed in response to RQ3 contains 5 elements: voter intimidation, conspiracies against civil rights, robocalls, fraudulent misrepresentations, and impediment of giving support or advocacy to candidates. Differences in applicable laws at the state and federal level show different scope of the laws. As a rule of thumb, they would only apply to deepfakes if they had a specific quality or characteristic like being about fundraising, being intimidating, or having a specific type of false statement. Voter intimidation laws, § 241, and laws prohibiting ads soliciting funds can all apply to deepfakes, while using § 1985(c) is most questionable.

---

[168] *See* Davis v. Cisneros, 744 F.Supp. 3d 696, 712 (W.D. Tex. 2024) ("The Reconstruction Congress intentionally differentiated 'support or advocacy' from the right to vote or other constitutional rights."); *see also, id.* at 714 ("The legislative history also demonstrates that in enacting the Klan Act, Congress's concerns were not limited to the narrow act of voting."). A more thorough investigation into this case is beyond the scope of this article.

[169] Anderson v. United States*,* 417 U.S. 211 (1974) (deceiving voters about which candidate was on the ballot).

[170] *Id.* at 226.

[171] *See* United States v. Saylor, 322 U.S. 385 (1944) (ballot stuffing); United States v. Classic, 313 U.S. 299 (1941) (ballot manipulation); United States v. Mosley, 238 U.S. 383 (1915) (omitting ballots).

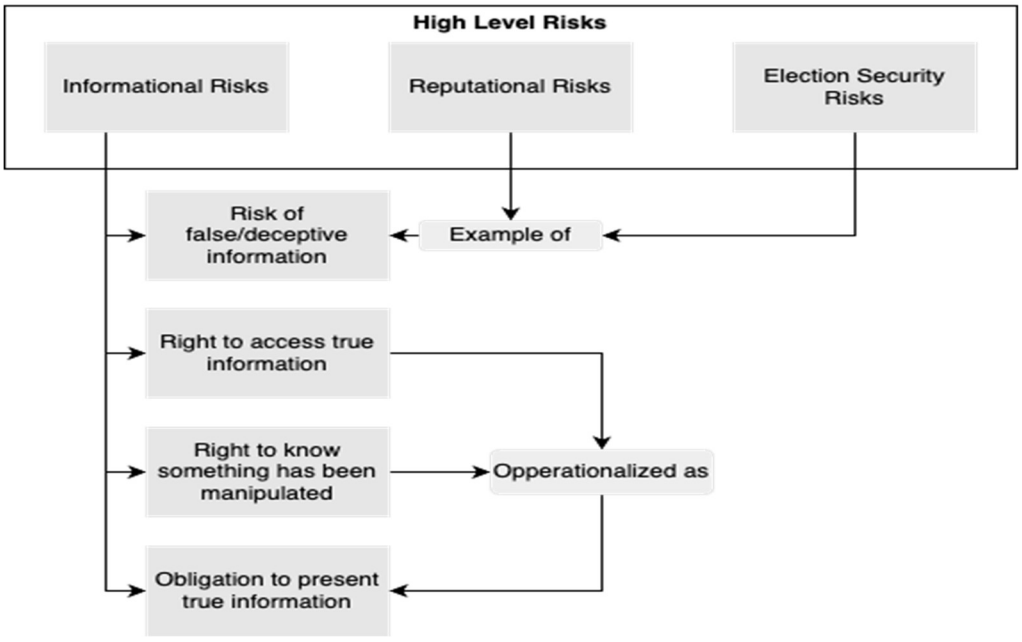
IV. RQ2: ANALYZING NEW LAWS

First, this Part analyzes the transcripts of committee hearings to identify the risks legislators envision new deepfake laws addressing. This process develops a theoretical risk model. Then I conduct a close reading of the enacted laws, assessing the risks they address. The laws address a slightly different set of risks. Testimony is mostly concerned with informational risks, with election security and reputational risks being given less emphasis. In contrast, the bills are heavily concerned with reputational risks to candidates.

A. Transcript Analysis

Three risks emerged from thematic analysis of 25 committee hearings: election security risks, reputational risks, and informational risks. I connect these risks together to form a theoretical risk model, pictured in Figure 1. Election security and reputational risks are simultaneously examples of subcomponents of informational risks: the risk of false and deceptive information. The other subcomponents are the right to access true information, the right to know something has been manipulated, and an obligation to present true information.

Figure 1: Risk Model From Testimony



1. Election Security Risks

First, election security risks concern the integrity of elections and ensuring they are free from foreign and domestic threats. For example,

California Assemblyman Berman referenced the Director of National Intelligence, the Select Committee on Intelligence, and foreign disinformation risks in three substantively identical speeches. [172] Indiana's Sen. Crane said, "[u]nfortunately people are going to do what they're going to do for nefarious purposes despite our best efforts . . . [we should] set up a system that elevates integrity and promotes the means by which the voter . . . can get the best information."[173] He focuses on addressing nefarious actors trying to impede election outcomes. These laws are seen as, "a win for voters and a win for the integrity of our process." [174] Some legislators even described deepfakes as outright forgeries harming election integrity. [175] Therefore, deepfakes heighten election security risks because they are fraudulent, have the potential to disrupt election integrity and can be used by foreign adversaries to influence elections.

2. Reputational Risks

Next, legislators frequently invoked "reputational risks" which concern harms to candidate's reputations and speech which is not theirs but is attributed to them. Committee discussion concerned other laws that could be used to mitigate deepfakes, harms to politicians' reputations, and what I term "uncontrolled speech". Politicians from states like Florida and Idaho discussed personal harm to other legislators during campaigns.[176] Committee members asked why defamation or libel

---

[172] *See Hearing on Assemb. B. 730 Before the Assemb. Comm. on Elections & Redistricting*, 2019-2020 Reg. Sess. (Cal. 2019) (statement of Assemb. Marc Berman, Member, Assemb. Comm. on Elections & Redistricting); *Hearing on Assemb. B. 730 Before the S. Judiciary Comm.*, 2019-2020 Reg. Sess. (Cal. 2019) (statement of Assemb. Marc Berman); *Hearing on Assemb. B. 730 Before the S. Elections & Constitutional Amendments Comm.*, 2019-2020 Reg. Sess. (Cal. 2019) (statement of Assemb. Marc Berman).

[173] *Hearing on H.B. 1133 Before the S. Election Comm.*, 123d Gen. Assemb., 2024 Reg. Sess. (Ind. 2024) (statement of Sen. John Crane, Member, S. Election Comm.).

[174] *Hearing on H.B. 5144 Before the H. Comm. on Elections*, 102d Leg., 2023-2024 Reg. Sess. (Mich. 2023) (statement of Rep. Matt Bierlein).

[175] *See id.* (statement of Rep. Penelope Tsernoglou, Chair, H. Comm. on Elections) ("As it continues to expand and a presidential election rapidly approaches, we have a duty to protect our elections and our democracy from misinformation and outright forgeries.").

[176] *See Hearing on H.B. 919 Before the H. Ethics, Elections & Open Gov't Subcomm.*, 126th Leg., 2024 Reg. Sess. (Fla. 2024) (statement of Rep. Alex Rizo, Member, H. Ethics, Elections & Open Gov't Subcomm.) ("[S]ince all of us are part of a political entity, if you will and all of us [sic] can, can campaign and do campaign at times. All of us are susceptible to any- any sort of image used with artificial intelligence that may be

laws were inadequate,[177] with bill sponsors explaining the standard is too high. [178] This consensus is supplemented with triangulation from committee reports with legal analysis from committee counsel.[179] I agree this barrier makes defamation ineffective at protecting legislators' reputations.

Reputational risks include "uncontrolled speech", defined as speech purporting to come from someone, but did not actually say it. The enactment of this speech causes associational harms to the depicted individual. Words appearing to come from one person's mouth are usually associated with them, but deepfakes falsify this purported association, harming the depicted individual. This focus on associational harm of speech is novel and deserves article length treatment, but an initial sketch of the harm will suffice.

Consider the cause-and-effect relationship between saying and doing. Politicians want to ensure, "voters [] know [their] opinions and not what someone else is falsely or maliciously putting forward on [them]."[180] Legislators personalized this risk. One noted, "[t]his could happen to anybody on this committee, a deepfake audio or video could be generated of you saying something, representing a position that you never took, that you never would say."[181]

Autonomy over the relationship between self-image and content produced with that image is central to the right of association. Violating this autonomy by making false association without consent is uncontrolled speech. Deepfakes have the potential to cause at least two injuries: lost autonomy over image and reputational damage due to

---

used for nefarious or negative reasons, and so."); *Hearing on H.B. 664 Before the H. State Affairs Comm.*, 2024 Reg. Sess. (Idaho 2024) (statement of Rep. Ilana Rubel, H. Min. Leader) ("I know he himself [my cosponsor] was a victim of artificially manipulated media in his last race, so this was matter's of concern to him as well.").

[177] *See, e.g., Hearing on H.B. 664 Before the H. State Affairs Comm.*, 2024 Reg. Sess. (Idaho 2024) (statement of Rep. Heather Scott, Member, H. State Affairs Comm.).

[178] *See, e.g., Hearing on H.B. 664 Before the H. State Affairs Comm.*, 2024 Reg. Sess. (Idaho 2024) (statement of Rep. Ilana Rubel, H. Min. Leader).

[179] *Compare* CAL. ELEC. CODE § 20500 (West) (applying defamation to candidates and political communications), *with* Cal. S. Judiciary Comm., Rep. on Assemb. B 730, at 11 (2019-2020 Reg. Sess.), (June 25, 2019) ("In California, a person can sue for false light when something highly offensive is implied to be true about that person when that thing is actually false. As public figures, candidates for office would probably have to show that the publication was made with actual malice [a harder and more difficult standard to reach].") (first citing *Gill v. Curtis Publishing Co.*, 38 Cal.2d 273 (1952); and then *Readers's Digest Ass'n v. Superior Court*, 37 Cal. 3d 244, 265 (1984)).

[180] *Hearing on H.B. 5144 Before the H. Comm. on Elections*, 102d Leg., 2023-2024 Reg. Sess. (Mich. 2023) (statement of Rep. Penelope Tsernoglou, Chair, H. Comm. on Elections).

[181] *Hearing on H.B. 664 Before the H. State Affairs Comm.*, 2024 Reg. Sess. (Idaho 2024) (statement of Rep. Ilana Rubel, H. Min. Leader).

content. Content – even made without consent – is not always (a positive deepfake could exist). However, autonomy violations are always present and injurious because they impede associational rights. Rep. Rubel articulated this distinction by creating (but not sharing) a deepfake of a colleague because if real, it might harm her colleague. In other words, "a corollary of the right to associate is the right not to associate."[182] Effectuating this right requires autonomy *a priori*, partly explaining why laws coercing association by all but requiring a form of association to win have been struck down.[183]

3. Informational Risks

a.) Risk of False/Deceptive Information

The risk of false/deceptive information occupies a central place in the theoretical model. It is the connection between election security and reputational risks because citizens must be able to believe what they see and hear their legislators doing. This indicates a connection between the two: the risk of false or misleading information. I argue legislators see election security and reputational risks as the consequences of false and misleading information. The extent of the risk of false and deceptive information is broad. Legislators fear misleading information will harm the election ecosystem and generate confusion.

The risk of false and deceptive information is an informational risk. This category encompasses three other components articulated below: the right to access true information, the right to know something has been manipulated, and the obligation to present true information.

---

[182] Cal. Democratic Party v. Jones, 530 U.S. 567, 574 (2000); *Cf.* Kim v. Hanlon, 99 F.4th 140, 151 (2024) (upholding a "constitutional right to not associate with other candidates" in the context of ballot placement).

[183] For example, the county line is a system that was used in New Jersey which required candidates to "bracket" or run on a joint ticket with other candidates. *See generally* Brett Pugach, *The County Line: The Law and Politics of Ballot Positioning in New Jersey*, 72 RUTGERS U. L. REV. 629 (2020) (explaining the county line system). A group of candidates running together had a visual advantage by being aligned together, which conveyed an average advantage of 38 points, compared to not being on the line. *See* Samuel S.-H. Wang, Hayden Goldberg & Julia Sass-Rubin, *Three Tests for Bias Arising from the Design of Primary Election Ballots in New Jersey*, 48 SETON HALL J. LEGIS. & PUB. POL'Y 24, 42 (2023). Moreover, "[n]o incumbent on the county line in all the counties in their district has lost a primary election since 2009 . . . [i]n contrast, in the other forty-nine states, 1,145 state legislative incumbents lost primary elections over that time period." Julia Rubin, *The Impact of New Jersey's County Line Primary Ballots on Election Outcomes, Politics, and Policy*, 48 SETON HALL J. LEGIS. & PUB. POL'Y 48, 57 (2023). This system was struck down for the 2024 Democratic Primary. *See Kim*, 99 F.4th at 147 (upholding the District Court's preliminary injunction to prohibit the use of the line).

The first two are on two sides of a similar, but not the same, coin. They emerge out of the risk of false/deceptive content and articulate rights legislators believe individuals ought to possess in the new campaign environment. The obligation to present true information is the operationalization of these rights.

b.) Right to Access True Information

Legislators argue citizens should have sufficient tools to evaluate information and determine if it is truthful. Ensuring information is truthful helps legislators ensure people believe what they see. Idaho's Rep. Rubel stated, "people can have *confidence in what they hear* and have some *faith that the information* they're being given when they see a candidate's face and voice, they can *know that that is what the person really said and did*."[184] Others framed this as a problem and imply the right is the solution to the problem, with Texas' Sen. Hughes saying, "each [person] is responsible to use our own filter to determine if what we read is reliable. Newer technology . . . could make it almost impossible for us to do that as voters, as participants, in democracy."[185] He believes the problem is that verifying information's truthfulness is too difficult, but people should retain agency to do it themselves. Put differently, this paternalistic goal ensures, "folks have time to sort out truth from fiction."[186]

Despite this emphasis on truthful information, the Liar's Dividend was never mentioned explicitly and infrequently alluded to. Only Robert Weissman (on behalf of Public Citizen) and Sen. Hughes of Texas alluded to it. The latter said, "[t]he advance of this technology would also make it very hard to hold someone accountable when they had committed a bad act because you wouldn't know if it was a deepfake or if the video was real."[187] Cumulatively, this demonstrates legislators envision a world where truth determination is too hard and their job is lowering the barrier.

c.) Right to Know Something Has Been Manipulated

Legislators argue a well-functioning democracy and a well-

[184] *Hearing on H.B. 664 Before the H. State Affairs Comm.*, 2024 Reg. Sess. (Idaho 2024) (statement of Rep. Ilana Rubel, H. Min. Leader) (emphasis added).
[185] *Hearing on S.B. 751 Before the S. Comm. on State Affairs (Part 1)*, 86th Leg., Reg. Sess. (Tex. 2019) (statement of Sen. Bryan Hughes, Vice Chair, S. Comm. on State Affairs).
[186] *Id.*
[187] *Id.*

informed public require voters to know if something has been manipulated. Access to information, which can facilitate debate, is routinely recognized by case law and democratic theorists as a central pillar of democracy.[188] Legislators framed knowing information had been manipulated as a cure to false and deceptive information because it widens the selection of speech voters can independently interpret. This is consistent with the market for information, a longstanding theoretical frame advanced by the Supreme Court.[189]

California Assemblyman Berman made this explicit, "I think we can all agree with the premise that voters have a right to know when video, audio, and images that they are being shown have been manipulated and do not represent reality to try to influence their vote in an upcoming election."[190] He reiterated this argument two months later.[191] He worries manipulated (and potentially false) images could injure voters by, "influencing the[ir] vote". This indicates the right derives from state's interest in ensuring voters are not unduly influenced. This focus on influence signals that we should look to other laws dealing with voter manipulation or influence to identify similar harms. By framing the right as an *a priori* necessity, he makes knowing information has been manipulated a baseline premise for constitutional democracy; the right cures some of the risks.

This concern was raised by others in the context of the risk of false and deceptive information. Rep. Arbit beseeched,

> [L]iberals and conservatives have very different views on how

---

[188] *See, e.g.,* New York Times Co. v. United States, 403 U.S. 713, 717 (1971) (Black, J., concurring) ("The press [is] protected so that it [can] bare the secrets of government and inform the people. Only a free and unrestrained press can effectively expose deception in government."); JOHN STUART MILL, ON LIBERTY 33 (1859) ("[T]he peculiar evil of silencing the expression of an opinion is, that it is robbing the human race; posterity as well as the existing generation; those who dissent from the opinion, still more than those who hold it. If the opinion is right, they are deprived of the opportunity of exchanging error for truth: if wrong, they lose, what is almost as great a benefit, the clearer perception and livelier impression of truth, produced by its collision with error.").

[189] For a review of the early history of this framework *see* ERIC T. KASPER & TROY A. KOZMA, THE SUPREME COURT AND THE PHILOSOPHER: HOW JOHN STUART MILL SHAPED US FREE SPEECH PROTECTIONS 45–62 (2024); *see also* Red Lion Broad. Co. v. F.C.C., 395 U.S. 367, 390 (1969) ("It is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail.").

[190] *Hearing on Assemb. B. 730 Before the S. Elections & Constitutional Amendments Comm.*, 2019-2020 Reg. Sess. (Cal. 2019) (statement of Assemb. Marc Berman).

[191] *Hearing on Assemb. B. 730 Before the Assemb. Elections & Redistricting Comm.*, 2019-2020 Reg. Sess. (Cal. 2019) (statement of Assemb. Marc Berman) ("I think we can all agree that voters have a right to know when video, audio and images that they're being shown have been manipulated and do not represent reality.").

> to organize our society . . . Our tolerance for coexistence depends on our ability to maintain at least some fidelity to shared reality. In a world where we cannot distinguish fact from fiction, truth from lies, our tether to reality to one another, to our shared democracy, will evaporate, leaving nothing but ruin.[192]

While her framing is partisan, she agrees with Berman on the need for a shared baseline reality. Both articulate the need for a baseline truth. Otherwise, democracy is at risk.

Other legislators tied this right into election integrity, focusing on ensuring voters have the information they need to independently evaluate the veracity of information. Legislators negotiated a balance between 1) a paternalistic desire to legislate truth and 2) upholding free speech norms which require individual agency. Sen. Crane of Indiana said this best, "I don't know that our responsibility is to try and control everything, but to do what we can do to at least set up a system that elevates integrity and promotes the means by which the voter downstream . . . can get the best information they need in order to make an informed decision." [193] By acknowledging the unpredictable "downstream" effects and raising other concerns over how responsibility should be split between legislators and public, the risk's scope is broadened. Mitigating this unpredictability in a crowded informational environment can be achieved by empowering citizens with the agency to verify information. Indiana's Rep. Olthoff viewed labeling as the best approach. She argued, "[i]f we require a disclaimer, campaign strategists may think twice about having to tell someone ads are not completely forthcoming."[194]

Michigan's Rep. Arbit begins articulating the boundaries of this right, saying it applies to the entire campaign apparatus, not just candidates or their direct agents. "[I]f you're not going to put a disclaimer on it, you're going to be penalized because you're basically trying [sic] to- to deceive voters and use that. And so what we're talking about is the apparatus is behind the campaign, [sic] the- the consultant network that

---

[192] *Hearing on H.B. 5144 Before the H. Comm. on Elections,* 102d Leg., 2023–2024 Reg. Sess. (Mich. 2023) (statement of Rep. Noah Arbit).
[193] *Hearing on H.B. 1133 Before the S. Election Comm.*, 123d Gen. Assemb., 2024 Reg. Sess. (Ind. 2024) (statement of Sen. John Crane, Member, S. Election Comm.).
[194] *Hearing on H.B. 1133 Before the S. Election Comm*., 123d Gen. Assemb., 2024 Reg. Sess. (Ind. 2024) (statement of H. Assistant Maj. Whip Julia Olthoff).

you know, conceived of . . . [and] distributed this."[195] In summary, the "goal [of this right] is to ensure that people know that the information is AI."[196]

d.) Obligation to Present True Information

To address these risks legislators operationalized these rights as an obligation for campaigns to present truthful information. New state laws seek to ensure "truth in campaign advertising."[197] Utah's goal was to "have better truth in advertising and campaigns." [198] This was operationalized by the law mandating "if something is altered the public needs to know that."[199] Washington's legislators aim to, "provid[e] ads that are truthful"[200] because "we need to ensure that we are keeping our democracy safe and ensuring that things are what they appear to be"[201] regardless of ad types and when they portray "a campaign or a position."[202]

This obligation for truth is not novel. Legislators discussed how the obligation has its roots in existing practices, resembling "stand by your ad laws" which require disclosing who paid for an ad to reduce negative advertising. Additionally, many states have laws mandating accurate ballot proposition summaries.[203]

---

[195] *Hearing on H.B. 5144 Before the H. Comm. on Elections,* 102d Leg., 2023–2024 Reg. Sess. (Mich. 2023) (statement of Rep. Noah Arbit).
[196] *Hearing on H.B. 919 Before the H. State Affairs Comm.*, 126th Leg., 2024 Reg. Sess. (Fla. 2024) (statement of Rep. Felicia Robinson, Member, H. State Affairs Comm.).
[197] *Hearing on S.B. 131 Before the S. Judiciary, L. Enforcement & Crim. Just. Comm.*, 65th Leg., 2024 Gen. Sess. (Utah 2024) (statement of Sen. Wayne Harper).
[198] *Hearing on S.B. 131 Before the H. L. Enforcement & Crim. Just. Comm.*, 65th Leg., 2024 Gen. Sess. (Utah 2024) (statement of Sen. Wayne Harper).
[199] *Id.*
[200] *Hearing on S.B. 5152 Before the S. State Gov't & Elections Comm.*, 68th Leg., 2023–2024 Reg. Sess. (Wash. 2023) (January 31, 2023) (statement of Sen. Valdez, Vice Chair, S. State Gov't & Elections Comm.).
[201] *Hearing on S.B. 5152 Before the S. State Gov't & Elections Comm.*, 68th Leg., 2023–2024 Reg. Sess. (Wash. 2023) (January 24, 2023) (statement of Sen. Valdez, Vice Chair, S. State Gov't & Elections Comm.).
[202] *Id.*
[203] For example, Eric Schor, Legislative Policy Director for the Department of State testified that "Michigan law already works very hard to ensure that our voters are informed, whether that's working through the process of the 100-word summary of a ballot question or putting those 'paid for by' disclaimers so we know who's behind other types of speech. And I think what's envisioned in these bills very much fits in with that line of thinking, of making sure that voters are making informed decisions." *Hearing on H.B. 5144 Before the H. Comm. on Elections*, 102d Leg., 2023–2024 Reg.

B. Textual Analysis of New State Deepfake Laws

Next, I examine the text of ten state deepfake laws. Broadly they create penalties for using unlabeled deepfakes in campaign ads, although two states prohibit them outright.[204] This is achieved in different ways. After reviewing the specific prohibitions, I analyze the impact of different legal philosophies including who can be harmed and how penalties are enforced; how "intent" language indicates risk; and the scope of the different laws. I argue this indicates the laws address different risks than the testimony, the focus shifts from the information environment to candidates.

To begin, state laws disagree on what is being prohibited. Texas outlaws "deep fake video[s]" which are "video[s], created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality."[205] In contrast, California prohibits "materially deceptive audio or visual media" while Washington prohibits "synthetic media" which covers "an image, an audio recording, or a video recording."[206] The definition matters beyond the term being defined; variation in the definition implies differences in risks being addressed. For example, Texas' law is restricted to video deepfakes so it could not be used for a fact pattern like *Kramer* which only concerns audio deepfakes.

1. Legal Philosophies

The laws reflect different legal philosophies, specifically in who is injured (standing) and what the penalties are. States vary in if they view violations as civil,[207] criminal,[208] or both.[209] These impact enforcement procedures and standards; for example, standing is only granted in civil cases. More generally, differences reflect variation in how states view the

---

Sess. (Mich. 2023) (statement of Erin Schor, Legis. Policy Director for the Michigan Department of State); *cf.* MICH. COMP. LAWS ANN. § 168.482b(2)(b) (West 2024) ("The summary is limited to not more than 100 words and must consist of a true and impartial statement.").

[204] *See* MINN. STAT. ANN. § 609.771 (West 2024), TEX. ELEC. CODE. ANN. § 255.004 (West).

[205] TEX. ELEC. CODE ANN. § 255.004(e) (West 2024).

[206] CAL. ELEC. CODE § 200109(a) (West 2024); WASH. REV. CODE ANN. § 42.62.020(1) (West).

[207] CAL. ELEC. CODE § 200109 (West 2024); WASH. REV. CODE ANN. § 42.62.020 (West 2024); IDAHO CODE ANN. § 67-6628A (West 2024); UTAH CODE ANN. § 20A-11-1104 (West 2024); IND. CODE ANN. § 3-9-8-6 (West 2024).

[208] WIS. STAT. ANN. § 11.1303 (West 2024); FLA. STAT. ANN. § 106.145 (West 2024); TEX. ELEC. CODE ANN. § 255.004(d) (West 2024).

[209] MICH. COMP. LAWS ANN. § 168.932f (West 2024); MINN. STAT. ANN. § 609.771 (West 2024).

harms caused by deepfakes. Civil injunctive relief means the harm occurs at sharing while criminal offenses emphasize harm at creation.

a.) Standing

In civil cases, a legal concept called "standing" – the ability to bring a lawsuit – varies. I argue choice to (not) give a party standing indicates how legislators envision the injury. While testimony focused on harms to candidates running for office and the public, the analysis below reveals the laws themselves focused mostly on reputational risks.

All states with civil penalties gave candidates standing. Table 1 provides three examples of how states differ.

Table 1: Conveyance of Standing

State	Michigan	Minnesota	Washington
Standing For	• Candidate • Attorney General • Depicted Individual • Organization that Represents Voters	• Candidate • Attorney General • Depicted Individual County or City Attorney	• Candidate

I suggest giving candidates standing ensures the campaign is being fought on equal footing with all members of the public having access to the truth. This finds analogues in federal court, where "competitor's standing" arises if a candidate alleges their opponent is not playing by the same rules.[210] When the state has standing through an agency or prosecutor, they represent the public. This is why criminal cases are captioned "State v. X" or "People v. X". State officers derive their power and authority from the people and represent their interests in criminal and civil matters. This interest allows states to intervene to "enforce and represent" their rights, as New York's Attorney General did

[210] *See* Nader v. Fed. Election Comm'n, 725 F.3d 226, 228 (D.C. Cir. 2013) ("Injury from an 'illegally structured' competitive environment can give rise to competitor standing.") (quoting LaRoque v. Holder, 650 F.3d 777, 787 (D.C. Cir. 2011)); Shays v. Fed. Election Comm'n, 414 F.3d 76, 85 (D.C. Cir. 2005) ("[I]llegal structuring of a competitive environment injures those who are regulated in that environment [and] longstanding precedent establishes that when a statute 'reflects a legislative purpose to protect a competitive interest, an injured competitor has standing to require compliance with that provision.'") (quoting Hardin v. Ky. Utils. Co., 390 U.S. 1, 6 (1968)) (cleaned up).

in *Wohl*.[211]

Giving the state but not individual citizens standing indicates risks to the state's interest in preserving the informational environment.[212] In contrast, citizens having standing implies they are harmed by lies, deception, and a misleading environment. Lawsuits are increasingly expensive, which is why organizations representing voters, but not voters themselves, bring lawsuits nowadays. However, Michigan is the only state granting organizations standing.[213]

These approaches of giving organizations and the state standing to represent the public resemble product liability and class action lawsuits. These entities represent the interests of the public or a large group of people who were harmed by false advertising.

b.) Penalties and Remedies

Broadly, penalties can be sorted into two buckets. First, criminal penalties prohibit the creation of deepfakes outright. Second, laws provide for civil relief via an injunction when a party is injured by a deepfake.[214] The details in how states vary within these buckets reveal the specific risks the laws address.

(1.) Texas and Criminal Intent

As a matter of common law, all criminal laws have a *mens rea* requirement.[215] Texas is the only state with criminal prohibitions to have *two* explicit intent requirements. The definition of "deep fake video" includes "intent to deceive."[216] An offense is committed, "if the person, with intent to injure a candidate or influence the result of an election"

---

[211] *See* Motion to Intervene by People of the State of New York at 1, Nat'l Coal. on Black Civic Participation v. Wohl, No. 1:20-cv-08668 (S.D.N.Y. May 6, 2021), ECF No. 97; *see also id.* at 2 (arguing the state has a "substantial interest in safeguarding the rights of New Yorkers who are threatened by unlawful voter intimidation.").

[212] *See* Eu, 489 U.S. at, 228–29.

[213] MICH. COMP. LAWS ANN. § 168.932f(4) (West).

[214] Injunctive relief is important in the voting rights context more broadly. *See* Delaney Herndon, *Voting Wrongs and Remedial Gaps*, 137 HARV. L. REV. 1182, 1195 (2024) ("The ability to seek preenforcement relief [of a harmful law] is crucial in the voting context, where elections are rarely rerun . . . Injunctions could prevent harm, not just to an individual plaintiff, but to everyone at risk of experiencing the same harm.").

[215] This applies even if a *mens rea* is not explicitly written into a statute. *See* Staples v. United States, 511 U.S. 600, 605 (1994) ("[W]e must construe the statute in light of the background rules of the common law in which the requirement of some *mens rea* for a crime is firmly embedded.") (internal citation omitted).

[216] TEX. ELEC. CODE ANN. § 255.004(e) (West) ("In this section, 'deep fake video' means a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality.").

creates a deepfake and shares it within 30 days of an election.[217] Therefore, intent must be demonstrated at creation and sharing. In contrast, other states require intent at only one of these stages. Importantly, this raises the bar for the type of conduct prohibited under the law. Voter intimidation laws' legislative history shows intent in civil election-law litigation is difficult to meet, let alone at the higher standard of evidence required in a criminal case.

Additionally, Texas' definition is unique by considering deepfakes a social phenomenon, not just a technological one. This indicates legislative concerns with their broad societal impacts, consistent with the social embedding of technology paradigm.[218] Requiring "intent to deceive" in the definition of a deepfake brings human behavior, norms, and goals into a technical definition. This contrasts with states like Idaho which are purely technical, partly defining deepfakes as, "created through the use of generative adversarial network techniques or other digital technology".

That is, Texas considers deception as part of its definition of a deepfake; deception occurs at the *creation* stage while most states incorporate deception at the *effects* stage of their analysis. This is concerning because laws are only as good as their scope and definitions articulate their scope. Texas' law is therefore much narrower because it requires demonstrating intent at creation (similar to the original voter intimidation laws) not at the sharing or effects stage (like section 11(b)).

While Texas law examines deepfakes outside a technology silo, it imposes a set of social values into the definition itself, further limiting the scope. Someone could make a deepfake of a candidate saying something benign. If other people believe it, that does not matter. What matters is the extent to which the *creator*'s intentions were there. While the law facially tries to protect citizens, its language shifts power and agency to creators; a jury's decision would hinge on the creator's intent, not if the viewer or candidate was harmed. This is counterintuitive because it reduces the law's usefulness practice, just like original voter intimidation law § 11(b) replaced. While not "protecting" creators nor authorizing them to make deepfakes, the law creates of grey area of coverage, which depends on a hard-to-prove mindset possessed by the

---

[217] TEX. ELEC. CODE ANN. § 255.004(d) (West).

[218] This framework originated in Trevor J. Pinch & Wiebe E. Bijker, *The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other*, 14 SOC. STUD. SCI. 399 (1984). For a more contemporary approach, *see* WIEBE E. BIJKER ET AL., THE SOCIAL CONSTRUCTION OF TECHNOLOGICAL SYSTEMS: NEW DIRECTIONS IN THE SOCIOLOGY AND HISTORY OF TECHNOLOGY (2012).

creator themselves. The law is much less friendly to those injured than initially appears.

(2.) Preliminary Injunctions

On the civil side, the main form of relief is a preliminary injunction. Getting a preliminary injunction requires showing a high likelihood of success on the merits.[219] Doing so immediately after filing a complaint usually requires strong evidence.

This creates a catch-22 for plaintiffs in deepfake lawsuits. Given the time sensitive nature of campaigns, these lawsuits will likely ask for injunctive relief (nearly) contemporaneous(ly) with filing the complaint, which is before discovery (the process of parties exchanging evidence) begins. Therefore, plaintiffs will be stuck between 1) waiting for evidence necessary for the injunction and 2) being harmed by the content they are seeking an injunction to prevent. While one could argue this is consistent with the extraordinary nature of injunctive relief, it is inconsistent with legislative testimony which emphasized the urgency and timeliness of harms and need to quickly grant relief.[220]

This is even more concerning in states where the law is only applicable 30-90 days before an election and/or have intent requirements written into them.[221] For example, California, Michigan, and Utah require showing intent when sharing deepfakes, meaning plaintiffs must have strong evidence specifically pointing to intent at the injunction stage. This could potentially create an insurmountable barrier

---

[219] Preliminary injunctions must meet a four part test defined in Winter v. Natural Resource Defense Council, Inc., 555 U.S. 7, 20 (2008) ("A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest."). In some circuits the "likely to succeed on the merits" criteria is weighed the most heavily. *See, e.g.*, Corp. Techs., Inc. v. Harnett, 731 F.3d 6, 9–10 (1st Cir. 2013) ("[L]ikelihood of success is the main bearing wall of the four-factor framework.") (internal citations and quotations omitted); Reilly v. City of Harrisburg, 858 F.3d 173, 179 (3d Cir. 2017) ("[A] movant for preliminary equitable relief must meet the threshold for the first two 'most critical' factors: it must demonstrate that it can win on the merits (which requires a showing significantly better than negligible but not necessarily more likely than not) and that it is more likely than not to suffer irreparable harm in the absence of preliminary relief."); *cf. see also* Samuel L. Bray, *The Purpose of the Preliminary Injunction*, 78 VAND. L. REV. (forthcoming 2025) (arguing the merits have become the dominant factor in preliminary injunction analysis).

[220] *See* Winter, 555 U.S. at 24 ("A preliminary injunction is an extraordinary remedy never awarded as of right.").

[221] *See, e.g.,* MICH. COMP. LAWS ANN. § 168.932f(1)(b) (West 2024) (law applies within 90 days of an election); TEX. ELEC. CODE ANN. § 255.004(d)(2) (West 2024) (law applies within 30 days of an election).

for plaintiffs in all but the most extreme cases because plaintiffs will not possess the necessary evidence in time for the remedy to be effective.

Kramer is an example of an extreme case based on media reports containing public statements admitting motive, which allowed a lawsuit and request for injunction to be filed quickly. But it took three months to hear the motion for a preliminary injunction, at which point the coverage of another state's laws might have already "expired". While an upcoming election may speed up this process due to clauses asking judges to fast-track cases,[222] this timeline remains a concern because it would mean the law is not achieving its purpose. Therefore, the laws may have inadvertently shot themselves in the foot by requiring a level of evidence for the main form of relief that is too high to be gathered on the timeline the law establishes.

2. "Intent" Indicates Risk

Regardless of if a law is criminal or civil, the different noun(s) articulating "intent to do what" articulate the risks being addressed. California and Washington require intentional manipulation of audiovisual material to be deepfake. Such intent can be shown with the mere creation of a deepfake, which requires active steps and consideration, making it least onerous intent requirement out of the explicit ones. Texas' intent requirement for deception was discussed above. Either way, intent requirements, especially involving "deception" remain harder to prove.

Some states include intent in their prohibitions, using language like intend to "injure a candidate",[223] "injure the candidate's reputation or to deceive a voter into voting for or against a candidate",[224] "harm the reputation or electoral prospects",[225] "change the voting behavior",[226] "influence voting",[227] "influence the result",[228] and "to influence voting for or against a candidate".[229] These can be sorted into three buckets.

First, "change the voting behavior", and "influence voting for or against a candidate" indicate a fear deepfakes are *the* reason a voter casts their ballot. States using the binary "for or against a candidate" ignore

---

[222] *See, e.g.,* IND. CODE ANN. § 3-9-8-6(d) (West 2024); WASH. REV. CODE ANN. § 42.62.020(6) (West 2024).
[223] FLA. STAT. ANN. § 106.145(2) (West 2024)
[224] CAL. ELEC. CODE § 20010(a) (West 2024).
[225] MICH. COMP. LAWS ANN. § 168.932f(1)(c) (West 2024).
[226] *Id.*
[227] UTAH CODE ANN. § 20A-11-1104(2)(b).
[228] MINN. STAT. ANN. § 609.771(2)(2) (West 2024).
[229] UTAH CODE ANN. § 20A-11-1104(2)(b).

the risk of deepfakes being used to persuade people to abstain from voting. Thus, broader language like intent to "influence voting" and "influence the result" better reflects how deepfakes could be used.

Second, intent to "harm the reputation or electoral prospects" of a candidate identifies reputational harms as a specific risk.[230] This harm is narrow and tangible; deepfakes can be identified as the reason someone changes their vote.

Thirdly, Florida uses a broad "injure" category, which can be subject to different interpretations and therefore risks. For example, Mackey argues deception is not an injury.[231] In contrast, scholar Rick Hasen argues denying voting rights and spreading misinformation about voting procedures is a tortious injury under common law.[232] "[I]njur[ing] a candidate" can include reputational damages and actions undermining people's ability give their support or advocacy.[233] Adopting Hasen's approach, "injure" is broader than the risks of state laws, covering substantive rights created by statute or the Constitution. I argue that uncontrolled speech is a substantive associational right conveyed by the Constitution and is violated by deepfakes. Accordingly, harms to associational rights caused by deepfakes are "injuries."

3. Scope

Finally, the laws vary in their scope, indicating different concerns with actors and timing. They are all limited to campaign ads and communications. While there are strong First Amendment reasons at common law for exceptions for parody, satire, and news reporting, not all states explicitly include them.[234]

Four states only enforce the laws in the lead up to elections. Michigan and Minnesota's laws apply within 90 days, California 60, and Texas 30.[235] Adding time limits recognizes the fact that, "[i]t is well

---

[230] MICH. COMP. LAWS ANN. § 168.932f(1)(c).
[231] *See* Opening Brief of Defendant-Appellant Douglass Mackey, *supra* note 132.
[232] Brief for Richard L. Hasen as Amicus Curiae Supporting Appellee and Affirmance at 5–9, United States v. Mackey, No. 23-7577 (2d Cir. Feb. 12, 2024), ECF 106.
[233] *Id*. at 5–9.
[234] On satire, *compare* Assemb. B. 730, 2019-2020 Reg. Sess. (Cal. 2019) (explicit exception) *with* Assemb. B. 664, 2023-2024 Leg., Reg. Sess. (Wis. 2024) (no explicit exception). *But compare* H.B. 664, 68th Leg., Reg. Sess. (Idaho 2024) (no explicit exception) *with Hearing on H.B. 664 Before the H. State Affairs Comm*., 2024 Reg. Sess. (Idaho 2024) (statement of Rep. Ilana Rubel, H. Min. Leader) (arguing the bill is not a threat to parody or satire). On news reporting, *compare* S.B. 5152, 68th Leg., Reg. Sess. (Wash. 2023) (explicit exemption for federally licensed broadcasters provided they do not remove the label) *and* Assemb. B. 730, 2019-2020 Reg. Sess. (Cal. 2019) (same) *with* H.B. 919, 126th Leg., Reg. Sess. (Fla. 2024) (no exception).
[235] MICH. COMP. LAWS ANN. § 168.932f(1)(b); CAL. ELEC. CODE § 20010(a); Tex. Elec.

known that the public begins to concentrate on elections only in the weeks immediately before they are held. There are short timeframes in which speech can have influence. The need or relevance of the speech will often first be apparent at this stage in the campaign. The decision to speak is made in the heat of political campaigns, when speakers react to messages conveyed by others."[236] Furthermore, "[t]hese requirements reflect 'the unique importance of the temporal window immediately preceding a vote,' when speech is more likely to be perceived as related to an election and the public is more likely to pay attention to and be affected by such speech."[237] That is, longer timelines reflect the "stickiness" of information and indicate the time period where people pay attention is longer.

One area of difference is how the laws view *where* someone is harmed. Uniquely, Utah's law considers second order, downstream effects. The law states, "a creator or sponsor who publishes [a deepfake] . . . that is viewable, audible, or accessible in the state shall ensure the advertisement carriers embedded tamper-evidence digital content provenance" that discloses additional information.[238] This recognizes that the internet does not respect borders and the ad's potential impact on people beyond the initial point of viewing. By mandating digital content provenance with edit history, the law seeks to mitigate confusion over the history of a particular ad. This resembles the concern raised in the *Citizens United* dissent regarding obfuscation of an ad's source.[239] Mandating the disclosure of the entities who modified the ad helps mitigate this risk.

This approach contrasts with Michigan, which is solely concerned with first-order effects. Its law only applies to entities "originally publish[ing] or originally distribut[ing]" a prohibited ad. It does not apply to people who reshare the ad.

This notion of first-and second-order effects is both theoretically and practically important. Civil injunctive relief is best positioned to mitigate second order and downstream effects by allowing those harmed

---

Code Ann. § 255.004(d)(2). Minnesota's law applies within 90 days of a nomination convention or after ballots have been sent out to voters. *See* MINN. STAT. ANN. § 609.771(2)(a)(3).

[236] Citizens United v. Fed. Election Comm'n, 558 U.S., at 334; *see also* New Georgia Project, Inc. v. Att'y Gen., State of Georgia, 106 F.4th 1237, 1251 (11th Cir. 2024) (citing *Citizens United* for this proposition).

[237] Nat'l Ass'n for Gun Rts. , Inc. v. Mangan, 933 F.3d 1102, 1117 (9th Cir. 2019) (quoting Hum. Life of Washington Inc. v. Brumsickle, 624 F.3d 990, 1019 (9th Cir. 2010)).

[238] UTAH CODE ANN. § 20A-11-1104(5).

[239] *See supra* note 44 and accompanying text.

to prohibit the further spread of deepfakes. While this results in a whack-a-mole in most instances, it acknowledges information transfer on the internet is not subject to state borders. First-order effects regarding creation are best targeted with criminal prohibitions to outlaw using deepfakes in political ads to begin with.

Finally, laws differ in if they prohibit "material deception" or "fabricated media." I argue fabrication is about the creation process, origin of the video, and source material. It concerns the originality and authenticity of the material at creation. In contrast, "material deception" is about the interpretation of the video. The risk is about voters being deceived and confused about the actual content of the video. This suggests different risks: one dealing with harm at creation and another at sharing. This strengthens the argument that laws view deepfake as harmful at creation and sharing. Additionally, it indicates they must balance viewing deepfakes as a technological risk and a social one.

4. Summary

In summary, this section has demonstrated laws addressed a different set of risks than ones articulated by legislative hearings. I have implicitly argued hearings were concerned about the reputational risks legislators suffered and the harm to the informational environment. Meanwhile, the conveyance of standing indicated an overarching concern for candidate injuries but a patchwork system for assisting voters. Furthermore, intent requirements (especially when requesting injunctive relief) have the potential to undermine laws by creating a catch-22 where evidence cannot be gathered fast enough to prove the injury to plaintiffs, preventing a remedy from being granted. Moreover, the election security risk of foreign interference was not explicitly addressed by the laws themselves.

C. RQ2 Risk Model

The analysis of hearings and state laws revealed a focus on risks to candidates, not voters. Legislators are concerned about how deepfakes could deceive the public with false information or by influencing their voting behavior. Laws varied regarding timeliness and how injured parties can seek relief. Differences in time before an election for where a law applies reflect how long legislators think information sticks in people's heads. However, labels are seen as a way to mitigate these harms because they inform the public that the content they are viewing is false. Finally, the laws were mostly concerned with risks to people's voting

behavior (in one form or another), while hearings articulated risks to the information environment and election security.

V. RQ1: PUTTING IT TOGETHER

Thus far, I have answered RQ2 and RQ3. Now I overlay the models to answer RQ1, "are new laws necessary?" I answer in the affirmative.

The lack of overlap indicates new laws are necessary because of a gap in the law. Therefore, these sets of laws deal with risks differing in kind, not of degree. This justifies the fundamentally new approach taken by contemporary laws.

The model developed for RQ3 focused heavily on impairment of voting rights and fraud, either through robocalls or representations. It centered how actors – especially during the civil rights and reconstruction eras – impinged on people's right to vote by creating roadblocks, either intentionally or through the effect of their actions. Other risks envisioned by specific state laws prohibiting misrepresentations were narrowly focused, and, in agreement with Rebecca Green, are insufficient to serve as a catch all prohibition.[240] Broadly these laws envisioned risks concerning effectuating the right to vote and preventing voter confusion about the source of campaign advertising.

These are differences in kind from the risks envisioned by new laws. Legislators envisioned new laws as addressing concerns about election security, reputational harms, and informational risks. They focused on ensuring citizens have access to true information and knowing something is false.

The concern, therefore, is on ensuring citizens have trust in the electoral system and its constituent components, with a big focus on the information environment. This contrasts with older laws focused on effectuating the right to vote and ensuring people seeking to vote could cast their ballot. Thus, old laws dealt with the act of voting itself, while new laws deal with the inputs into the act: the information environment.

The most overlap is seen with fraudulent misrepresentations and ensuring ads are what they appear to be. However, old laws focused on specific factual circumstances of what is contained within an ad, while new laws are intended to address the information environment at large.

---

[240] See Green, *supra* note 74, at 1470–71 ("Commonly, state election codes feature highly-specific bans such as prohibitions on stating endorsements falsely, misrepresenting the origin of a telephone call, or misrepresenting a candidate's voting record, none of which would cover counterfeited campaign speech unless it related to a prohibited category.").

Despite some overlap, deepfakes present a broader set of risks spanning the entire content of an ad. This means old laws do not adequately address the entire risk model, since they only address specific elements of a subset of ads (intimidation, solicitation, and certain factual statements). This makes new laws necessary.

Importantly, the old laws nearly completely fail to address reputational risks and election security risks; the former is critical to the text of the laws. While the fraudulent misrepresentations law can instigate investigations into frauds and reveal the true source of information, thereby clarifying the information environment, this process is not reliable and only applies in a limited set of circumstances. It neither addresses foreign election interference nor increases citizens' faith in the election's integrity. Meanwhile, legislators and legal scholarship devoted significant attention to a gap in defamation law, which has too high of a standard to be useful in campaigns.

However, this reveals another limitation to new laws: they only address campaign communications. While old laws are effective at various stages of the elections process –including from voter registration. ballot casting, fundraising, and political engagement – the newer laws focus specifically on campaign ads and communications from authorized sources. Additionally, older laws applied to all citizens engaging in the prohibited behavior, regardless of whether they were a registered or a legally recognized entity. In contrast, newer laws only apply to political entities, and their standing requirements indicate harms apply to candidates and only a select few others, which varies by state.

Finally, old laws only address first-order effects like intimidation by solely applying to the people directly impacted by content. Deepfakes are unrestrained by geography, opening a new dimension of second order risks old laws cannot handle.

CONCLUSION

States with deepfake prohibition laws are insufficiently protected because the laws impose too high of a bar to be effective at mitigating all the risks. Yet legislators and citizens may think they are adequately protected, unaware the entire risk was not addressed. In the states without these laws, these findings indicate passing new laws in the next legislative session is necessary to fill large gaps in the law. States can learn from these findings to strike a balance between being narrowly tailored and effective.

First, injunctive relief is the best option because deepfakes can

impact elections by damaging reputations and the information environment. The one-off nature of elections and the outcome of being elected (or not) means monetary damages or specific performance (a court order to follow a contract) do not address the harms caused to candidates or voters. In practice, it is likely difficult to assess if a single deepfake swayed an election. Additionally, candidates should be able to get relief from a harmful deepfake, even if they win the election. This leaves injunctive relief as the best remaining remedy. In light of these findings, states should write into the statute a lower evidentiary requirement and/or specify a different test for granting preliminary injunction than the one traditionally used.[241]

Second, states should give standing to organizations and local officials. Widening standing acknowledges the breadth of who can be harmed by unlabeled deepfakes. Organizations with a track record of working with voters are well suited to represent these interests at large. They should be granted standing, following Michigan's example.

However, such entities are unlikely to be aware of everything happening locally, necessitating standing requirements for district attorneys and city attorneys. In this respect, deepfakes are similar to political mailers. In "low information" elections voters are usually uninformed about candidates. Thus, a snappy smear campaign in a local election could be effective because there is no local media to discredit it. Mailers and deepfakes are both cheap and easy to disseminate. This creates another catch-22: the elections where deepfakes could have the largest impact (local, low information elections) are also the ones most lacking adequate counter-speech mechanisms (the death of local news in America, which could report on the falsity of the deepfake).[242] Moreover, candidates in these elections are unlikely to have sufficient funding to bring lawsuits themselves. Thus, local officials like district and city attorneys should be granted standing, filling this gap.

On the whole, to truly mitigate the potential harms of deepfakes, a more comprehensive, whole-of-government approach is likely to be necessary.[243] However, states are well placed to lead this approach and learn from these findings.

---

[241] *See* Winter, 555 U.S. at, 20.

[242] On the decline of local news, *see, e.g.,* Sarah Naseer & Christopher St. Aubin, *Newspapers Fact Sheet*, (Nov. 10, 2023), https://www.pewresearch.org/journalism/fact-sheet/newspapers/#economics.

[243] For more on the whole of government approach, *see* Hayden Goldberg, *Public Comment on Disclosure and Transparency of Artificial Intelligence-Generated Content in Political Advertisements*, FCC Docket 24-211, at 12–13 (Sept. 16, 2024).

APPENDIX 1: STATE BILLS AND LAWS

Each state bill considered in this article was passed and enacted. The Bluebook Rule 13.2(b) proscribes citing to the statute if a bill has been enacted, unless discussing legislative history in which case the bill may be citied. Based on context, the footnotes cite to either the statute or bill. Table A2.1 below can be used as a reference to link the bill, statute, and committee hearings in which it was held.

Table A2.1: State Bills and Accompanying Laws

State	Bill	Statute
California	A.B. 730, 2019-2020 Reg. Sess. (Cal. 2019)	Cal. Elec. Code § 20010 (West)
Florida	H.B. 919, 126th Leg., Reg. Sess. (Fla. 2024)	Fla. Stat. Ann. § 106.145 (West)
Idaho	H.B. 664, 68th Leg., Reg. Sess. (Idaho 2024)	Idaho Code Ann. § 67-6628A (West)
Indiana	H.B. 1133, 123rd Gen. Assemb., Reg. Sess. (Ind. 2024)	Ind. Code Ann. § 3-9-8-1 (West) Ind. Code Ann. § 3-9-8-2 (West) Ind. Code Ann. § 3-9-8-3 (West) Ind. Code Ann. § 3-9-8-4 (West) Ind. Code Ann. § 3-9-8-4 (West) Ind. Code Ann. § 3-9-8-5 (West) Ind. Code Ann. § 3-9-8-6 (West) The bill created five discrete sections of Indiana code, all numbered sequentially.
Michigan	H.B. 5144, 102nd Leg., Reg. Sess. (Mich. 2023)	Mich. Comp. Laws Ann. § 168.932f (West)
Minnesota	H.F. 1370, 93rd Leg., Reg. Sess. (Minn. 2023)	Minn. Stat. Ann. § 609.771 (West)
Texas	S.B. 751, 86th Leg., Reg. Sess. (Tex. 2019)	Tex. Elec. Code Ann. § 255.004 (West)
Utah	S.B. 131, 65th Leg., Gen. Sess. (Utah 2024)	Utah Code Ann. § 20A-11-1104 (West)
Washington	S.B. 5152, 68th Leg., Reg. Sess.	Wash. Rev. Code Ann. § 42.62.020 (West)

	(Wash. 2023)	
Wisconsin	A.B. 664, 2023-2024 Leg., Reg. Sess. (Wis. 2024)	Wis. Stat. Ann. § 11.1303 (West)

APPENDIX 2: COMMITTEE HEARING INFORMATION

Across the 10 states, the bills were heard in a total of 25 hearings. These relevant portions of hearings totaled 458 minutes (7 hours, 38 minutes) and the total length of all hearings was 3462 minutes (57 hours, 42 minutes). By "relevant" I mean the portion of the hearing covering the bill.

Table A3.1 provides summary information about the number of hearings and their length on a state by state basis.

Table A3.1: Committee Hearings Summary

State	Hearings	Relevant Portion Length (minutes)	Total Length (minutes)
CA	3	42	819
FL	3	49	344
ID	2	22	100
IN	2	48	327
MI	2	128	153
MN	3	39	233
TX	2	22	366
UT	2	22	166
WA	4	56	335
WI	2	30	619

Table A3.2 (below) contains metadata about each hearing, including the state, bill, committee, date it took place, transcription method used for that hearing, total length of the hearing in minutes, and portion of the hearing devoted to consideration of the relevant bill.

Table A3.2: Committee Hearing Details

State	Bill	Hearing	Date	Transcription Method	Relevant Length	Full Length
CA	AB 730	Assembly Committee on Elections and Redistricting	13-Sep-19	Manual verification of word transcription of mp3	6	21
CA	AB 730	Senate Committee on Judiciary	9-Jul-19	Manual verification of state provided transcript	15	653
CA	AB 730	Senate Committee on Elections and Constitutional Amendments	2-Jul-19	Manual verification of state provided transcript	21	145

FL	HB 919	House Ethics, Elections & Open Government Subcommittee	18-Jan-24	Manual verification of word transcription of mp3	18	34
FL	HB 919	House Justice Appropriations Subcommittee	29-Jan-24	Manual verification of word transcription of mp3	5	78
FL	HB 919	House State Affairs Committee	14-Feb-24	Manual verification of word transcription of mp3	26	232
ID	HB 664	House State Affairs	4-Mar-24	Quick time player exported as audio only file, followed by manual verification of Word transcription	15	50
ID	HB 664	Senate State Affairs	11-Mar-24	Quick time player exported as audio only file, followed by manual verification of Word transcription	7	50
IN	HB 1133	House Committee on Elections and Apportionment	17-Jan-24	Manual transcription	8	173
IN	HB 1133	Senate Election Committee	12-Feb-24	Manual transcription	40	154
MI	HB 5144	House Committee on Elections	17-Oct-23	Quick time player exported as audio only file, followed by manual verification of Word transcription	81	81
MI	HB 5144	Senate Committee on Elections and Ethics	8-Nov-23	Quick time player exported as audio only file, followed by manual verification of Word transcription	47	72
MN	HF 1370	House Elections Finance and Policy Committee	15-Feb-23	Quick time player exported as audio only file, followed by manual verification of Word transcription	21	49
MN	HF 1370	House Judiciary Finance and Civil Law Committee	2-Mar-23	Quick time player exported as audio only file, followed by manual verification of Word transcription	12	83
MN	HF 1370	House Public Safety Finance and Policy	9-Mar-23	Quick time player exported as audio only file, followed by	6	101

				manual verification of Word transcription		
TX	SB 751	House Committee on Elections	6-May-19	Manual transcription	5	94
TX	SB 751	Senate Committee on State Affairs (Part 1)	1-Apr-19	Manual transcription	17	272
UT	SB 131	House Law Enforcement and Criminal Justice Committee	21-Feb-24	Manual transcription	12	67
UT	SB 131	Senate Judiciary, Law Enforcement, and Criminal Justice Committee	31-Jan-24	Manual transcription	10	99
WA	SB 5152	Senate State Government and Elections	24-Jan-23	Manual transcription	14	84
WA	SB 5152	Senate State Government and Elections	31-Jan-23	Manual verification of state provided transcript	8	103
WA	SB 5152	House State Government and Tribal Relations	10-Mar-23	Manual verification of state provided transcript	19	111
WA	SB 5152	House State Government and Tribal Relations	29-Mar-23	Manual verification of state provided transcript	15	37
WI	AB 664	Assembly Committee on Campaigns and Elections	9-Jan-24	Manual verification of state provided transcript	24	379
WI	AB 664	Assembly Committee on Campaigns and Elections	30-Jan-24	Manual verification of state provided transcript	6	240