



Fall 12-1-2021

"Malicious Deepfakes" - How California's A.B. 730 Tries (and Fails) to Address the Internet's Burgeoning Political Crisis

Alexandra Tashman

Follow this and additional works at: <https://digitalcommons.lmu.edu/llr>

Recommended Citation

Alexandra Tashman, *"Malicious Deepfakes" - How California's A.B. 730 Tries (and Fails) to Address the Internet's Burgeoning Political Crisis*, 54 Loy. L.A. L. Rev. 1391 (2021).

Available at: <https://digitalcommons.lmu.edu/llr/vol54/iss4/8>

This Notes is brought to you for free and open access by the Law Reviews at Digital Commons @ Loyola Marymount University and Loyola Law School. It has been accepted for inclusion in Loyola of Los Angeles Law Review by an authorized administrator of Digital Commons@Loyola Marymount University and Loyola Law School. For more information, please contact digitalcommons@lmu.edu.

“MALICIOUS DEEPPAKES”—HOW CALIFORNIA’S A.B. 730 TRIES (AND FAILS) TO ADDRESS THE INTERNET’S BURGEONING POLITICAL CRISIS

*Alexandra Tashman**

I. INTRODUCTION

Alternative facts are not facts; they’re falsehoods.

—Chuck Todd, in response to Kellyanne Conway on NBC’s *Meet the Press*.¹

In today’s era of “fake news,” there are a myriad of ways to make what is false seem entirely real. The proliferation of half-truths, mistruths, and un-truths is no longer constrained to the realm of yellow journalists and tabloids; rather, anyone from the nation’s most powerful figures to conspiracy theorist bloggers can generate a national controversy out of nothing. This shift has not occurred in a vacuum. Instead, technology has been the engine driving change in what becomes news, who creates news, and how news reaches the public.

The central legal problem surrounding the astounding rate of technological developments is that they constantly outpace any regulatory attempts to constrain them.² This is true broadly, but it keenly applies in the context of manipulated media—commonly

* J.D. Candidate, May 2021, Loyola Law School, Los Angeles; B.A. History and Political Science, University of California, Los Angeles, September 2015. Sincere thanks to Professor Rebecca Delfino for the inspiration and advice. Thank you as well to my dear friends Savannah Badalich and Adam Drown for being my sounding boards, and for guiding me through the technical aspects of writing this Note. And finally, thank you to my parents, sister, grandparents, and friends for their unflinching and unconditional support.

1. NBC News, *Kellyanne Conway: Press Secretary Sean Spicer Gave ‘Alternative Facts’ | Meet the Press | NBC News*, YOUTUBE (Jan. 22, 2017), <https://www.youtube.com/watch?v=VSrEEDQgFc8>.

2. Julia Griffith, *A Losing Game: The Law Is Struggling to Keep Up with Technology*, J. HIGH TECH. L. (Apr. 12, 2019), <https://sites.suffolk.edu/jhtl/2019/04/12/a-losing-game-the-law-is-struggling-to-keep-up-with-technology>.

referred to as “deepfakes.”³ Deepfakes are “highly realistic and difficult-to-detect digital manipulations of audio or video.”⁴ The word is a portmanteau of “deep learning” and “fakes,” which together roughly encapsulate what the technology is.⁵ The name can also be traced back to a Reddit⁶ user, who went by the name “deepfakes,” and was the first to widely disseminate the technology in 2017 (as a means of spreading nonconsensual pornography).⁷ Part of what makes this technology so insidious is that there is no one “type” of deepfake. *The Washington Post* has attempted to sort deepfakes into three categories: those that involve “missing context” (which includes misrepresentation and isolation of clips), those which use “deceptive editing” techniques (which use omissions and splicing), and videos that have undergone “malicious transformation” (which involves doctoring and fabricating footage).⁸ These videos can run the gamut from silly (like a viral clip of actor Steve Buscemi’s head on actress Jennifer Lawrence’s body)⁹ to terrifying, and can include videos manipulated for political gain, national security threats, and revenge pornography.¹⁰ What makes deepfakes even more disconcerting is that it is often hard to tell—especially at first glance—whether a video is manipulated or authentic.¹¹ Subsequently, even the most erudite of

3. Nadine Ajaka et al., *Seeing Isn't Believing: The Fact Checker's Guide to Manipulated Video*, WASH. POST (June 25, 2019), <https://www.washingtonpost.com/graphics/2019/politics/fact-checker/manipulated-video-guide> [<https://web.archive.org/web/20201217114615/https://www.washingtonpost.com/graphics/2019/politics/fact-checker/manipulated-video-guide/>].

4. Robert Chesney & Danielle Citron, *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics*, FOREIGN AFFS., Jan./Feb. 2019, at 147, 147–48.

5. Rebecca A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*, 88 FORDHAM L. REV. 887, 890 n.5 (2019).

6. Matt Silverman, *Reddit: A Beginner's Guide*, MASHABLE (June 6, 2012), <https://mashable.com/2012/06/06/reddit-for-beginners>. Reddit is an internet platform designed to allow users to share videos, images, and stories which are spread to a greater (or fewer) number of viewers through the number of “upvotes” (positive endorsements) or “downvotes” (negative endorsements) a post receives. *Id.*

7. Delfino, *supra* note 5, at 893; James Vincent, *Why We Need a Better Definition of 'Deepfake'*, THE VERGE (May 22, 2018, 2:53 PM), <https://www.theverge.com/2018/5/22/17380306/deepfake-definition-ai-manipulation-fake-news>; Samantha Cole, *We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now*, VICE: MOTHERBOARD (Jan. 24, 2018, 10:13 AM), https://motherboard.vice.com/en_us/article/bjye8a/reddit-fake-porn-app-daisy-ridley.

8. Ajaka et al., *supra* note 3.

9. Delfino, *supra* note 5, at 897.

10. *See generally* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1776 (2019) (detailing the dangers that deepfake technology will pose to society, using politics, national security, and revenge pornography as examples).

11. *Id.* at 1758–59.

news consumers (and perhaps more crucially, political officials) can fall prey to what these types of videos purport to depict.

The spread of deepfakes is particularly alarming as it applies to the democratic process. Altered videos have already begun to make a substantial impact on the American political psyche, as the nation has come to place its trust in video news (a quarter of modern Americans now obtain the bulk of their news from YouTube).¹² Consequently, deepfake videos have the potential to create devastating ramifications. Deepfake videos “could feature public officials taking bribes, displaying racism, or engaging in adultery. Politicians and other government officials could appear in locations where they were not, saying or doing things that they did not.”¹³ The FBI has expressed serious concern about these possibilities, noting in a March 2021 bulletin that malicious foreign actors have already begun to use “synthetic content” in influence campaigns.¹⁴ Further, the Carnegie Endowment for International Peace even asserts that deepfakes “have the potential to incite violence, alter election outcomes, and undermine diplomacy.”¹⁵ These warnings are not merely hypothetical. Deepfake videos have already become impactful in the electoral context. For example, many of former President Donald Trump’s supporters believed his January 7, 2021, concession video was in fact a deepfake (it was not).¹⁶ Political manipulation via deepfake even transcends national borders. In April 2021, Dutch politicians were tricked on a live video call by an impersonator using deepfake technology to

12. Sarah Perez, *A Quarter of US Adults Now Get News from YouTube*, *Pew Research Study Finds*, TECHCRUNCH (Sept. 28, 2020, 9:00 AM), <https://techcrunch.com/2020/09/28/a-quarter-of-u-s-adults-now-get-news-from-youtube-pew-research-study-finds>.

13. Chesney & Citron, *supra* note 10, at 1776.

14. U.S. DEP’T OF JUSTICE, FED. BUREAU OF INVESTIGATION, MALICIOUS ACTORS ALMOST CERTAINLY WILL LEVERAGE SYNTHETIC CONTENT FOR CYBER AND FOREIGN INFLUENCE OPERATIONS (2021), <https://www.ic3.gov/Media/News/2021/210310-2.pdf>; see also Glenn Gow, *The Scary Truth Behind the FBI Warning: Deepfake Fraud Is Here and It’s Serious—We Are Not Prepared*, FORBES (May 2, 2021, 6:00 AM), <https://www.forbes.com/sites/glenngow/2021/05/02/the-scary-truth-behind-the-fbi-warning-deepfake-fraud-is-here-and-its-serious-we-are-not-prepared/> (“Another phrase for ‘synthetic content’ is deepfake content.”).

15. *Elections: Deceptive Audio or Visual Media, Third Reading of Assembly Bill No. 730 Before the S. Rules Comm.*, 2019–2020 Reg. Sess. 6 (Cal. 2019) (as amended Aug. 13, 2019).

16. Daniel Villarreal, *Parler Users Call Trump’s Concession Video ‘Deep Fake,’ and Worry He’ll ‘Sell Us Out,’* NEWSWEEK (Jan. 7, 2021, 11:59 PM), <https://www.newsweek.com/parler-users-call-trumps-concession-video-deep-fake-worry-hell-sell-us-out-1559895>.

appear as Leonid Volkov, chief of staff to Russian opposition leader Alexei Navalny.¹⁷

Managing the spread of this form of disinformation also presents logistical and technological challenges. Video authentication technology remains in its infancy and is not easy to do either quickly or cheaply.¹⁸ Even as that technology develops, it is being exploited to improve the quality of deepfakes themselves.¹⁹ With few tangible methods available to establish veracity, these types of deepfakes will only continue to impact the outcomes of campaigns and elections.

It is for this reason, among many others, that lawmakers have begun actively trying to find ways to legislate the creation and proliferation of so-called “malicious” deepfakes.²⁰ Unsurprisingly, they have encountered a series of obstacles. In part, this is because many lawmakers have a limited understanding of cutting-edge technology and are conflicted on how to regulate it effectively.²¹ Plus, the regulation of media, no matter how harmful to society that media may have the potential to be, rings alarm bells for free speech advocates of all political persuasions.

At the forefront of this issue is California Assembly Bill No. 730 (“A.B. 730”).²² Passed by the California State Legislature in September 2019 and signed into law by Governor Gavin Newsom in October of that year, the law attempts to address the potential impact of deepfakes on the democratic process by amending California’s existing elections code.²³ The new law

prohibit[s] a person, committee, or other entity, within 60 days of an election at which a candidate for elective office will appear on the ballot, from distributing with actual malice

17. J. Fingas, *Dutch Politicians Were Tricked by a Deepfake Video Chat*, ENGADGET (Apr. 24, 2021), <https://www.engadget.com/netherlands-deepfake-video-chat-navalny-212606049.html>.

18. Chesney & Citron, *supra* note 10, at 1785.

19. Hengtee Lim, *The Best (and Worst) Deepfakes Developments in 2020*, LIONBRIDGE (Oct. 5, 2020), <https://lionbridge.ai/articles/a-look-at-deepfakes-in-2020/> [<https://web.archive.org/web/20201106084900/https://lionbridge.ai/articles/a-look-at-deepfakes-in-2020/>] (“[D]eepfake detection models can also be used to improve deepfake creation algorithms.”).

20. David Ruiz, *Deepfakes Laws and Proposals Flood US*, MALWAREBYTES LABS (Jan. 23, 2020), <https://blog.malwarebytes.com/artificial-intelligence/2020/01/deepfakes-laws-and-proposals-flood-us/>.

21. Cecilia Kang et al., *Knowledge Gap Hinders Ability of Congress to Regulate Silicon Valley*, N.Y. TIMES (Apr. 12, 2018), <https://www.nytimes.com/2018/04/12/business/congress-facebook-regulation.html>.

22. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

23. *Id.*

materially deceptive audio or visual media of the candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate.²⁴

The purpose behind this policy, as outlined by the law's sponsor, California State Assemblymember Marc Berman, is to diminish the impact of "those who want to wage misinformation campaigns to confuse voters."²⁵

The intentions behind the passage of A.B. 730 appear noble—digital manipulation can impact elections and elected officials, and it often presents terrifyingly dystopian implications. This law is especially relevant, as deepfakes have already made substantial waves in the political sphere. The most high-profile instance yet of a political deepfake was a May 2019 video of Speaker of the House Nancy Pelosi, which was slowed down and distorted to make her seem drunk and disoriented.²⁶ The video quickly went viral, racking up millions of views overnight, with no mechanism in place to indicate to viewers that it was false.²⁷ The creator of the video, naturally, remains unknown. At the time, Facebook²⁸ was widely criticized for refusing to remove or disclaim the video, allowing it to have broader reach (without indicating its falsity).²⁹ The social media giant and its fellows have since implemented new policies to combat deepfakes,³⁰ but

24. *Id.*

25. Levi Sumagaysay, *California Has a New Deepfakes Law in Time for 2020 Election*, MERCURY NEWS (Oct. 4, 2019, 3:14 PM), <https://www.mercurynews.com/2019/10/04/california-has-a-new-deepfakes-law-in-time-for-2020-election/>.

26. Shirin Ghaffary, *Facebook Is Banning Deepfake Videos*, VOX: RECODE (Jan. 7, 2020, 1:15 PM), <https://www.vox.com/recode/2020/1/7/21055024/facebook-ban-deepfake-video>.

27. Emily Stewart, *A Fake Viral Video Makes Nancy Pelosi Look Drunk. Facebook Won't Take It Down*, VOX: RECODE (May 24, 2019, 3:50 PM), <https://www.vox.com/recode/2019/5/24/18638822/nancy-pelosi-doctored-video-drunk-facebook-trump>.

28. Facebook is an online social media platform where users can add people they know as "friends" and share news, information, articles, photos, and videos. See Chaim Gartenberg, *What Is Facebook? Just Ask Mark Zuckerberg*, THE VERGE (Mar. 8, 2019, 9:00 AM), <http://theverge.com/2019/3/8/18255269/facebook-mark-zuckerberg-definition-social-media-network-sharing-privacy> (noting that "Facebook has grown from a site where people in colleges would accept each other as friends to one of the biggest and most influential companies in the entire world, one with billions of users and the power to affect political landscapes around the globe").

29. Stewart, *supra* note 27; see also Angela Chen, *Why Facebook Is Right Not to Take Down the Doctored Pelosi Video*, MIT TECH. REV. (May 28, 2019), <https://www.technologyreview.com/2019/05/28/103039/facebook-pelosi-video-misinformation-censorship-free-speech/> ("Critics are condemning Facebook for not taking down a video of House Speaker Nancy Pelosi that was slowed to make her seem drunk. But some experts argue that removing the video might have set a precedent that would actually cause more harm.")

30. *Id.*

legislative efforts like A.B. 730 are attempting to circumvent forced reliance on independent social media platforms by offering tangible, legal solutions instead. The problem with A.B. 730, however, lies in the feebleness of those solutions.

First and foremost, A.B. 730 is redundant. It creates a separate cause of action for issues which can already be addressed through California's extant defamation laws, which are better settled and more clearly defined. Potential litigants could also utilize the state's false light and right of publicity statutes to greater effect. None of these areas of law require the same stringent time and methodology requirements as A.B. 730, and all offer a broader library of caselaw for litigants to turn to.

Second, A.B. 730 presents serious constitutional implications, as it contradicts a number of Supreme Court rulings on the First Amendment, particularly as it relates to both political and anonymous speech. Laws that limit political speech (however misleading that speech may be), are held to the highest degree of judicial scrutiny.³¹ A.B. 730 could face challenges for a lack of content neutrality, as well as for not "provid[ing] other options for communicating the message [contained in the deepfake]."³² The United States Supreme Court has previously held that a "State's fear that voters might make an ill-advised choice does not provide the State with a compelling justification for limiting speech."³³ As a result, "courts therefore have struck down periodic attempts to ban election-related lies," which deepfakes are a form of.³⁴

Finally, and perhaps most crucially, A.B. 730 has an almost insurmountable feasibility problem. It does not matter whether malicious deepfakes are technically illegal if their creators cannot be located or held accountable. Bad actors who are sophisticated enough to be developing realistic political deepfakes are likewise sophisticated enough to use encrypted browsers and other means of technological subterfuge.³⁵ These users' ability to cover their tracks makes the law functionally unenforceable. A.B. 730 also places an

31. 13 CAL. JUR. 3D *Constitutional Law* § 254, Westlaw (database updated Feb. 2021).

32. Holly Kathleen Hall, *Deepfake Videos: When Seeing Isn't Believing*, 27 CATH. UNIV. J.L. & TECH. 51, 63 (2018).

33. *Brown v. Hartlage*, 456 U.S. 45, 46 (1982); Chesney & Citron, *supra* note 10, at 1803.

34. Chesney & Citron, *supra* note 10, at 1803.

35. Andy Greenberg, *It's About to Get Even Easier to Hide on the Dark Web*, WIRED (Jan. 20, 2017, 7:00 AM), <https://www.wired.com/2017/01/get-even-easier-hide-dark-web>.

enormous burden on litigants due to its intent standard, which requires they prove “actual malice” in the distribution of the manipulated media.³⁶ It also places legal responsibility on the individuals who create the deepfakes, rather than on the platforms which enable their spread, by carving out an exception for service providers under Section 230 of the Communications Decency Act.³⁷ The law also limits its own strength with a sunset clause, which makes it enforceable only through 2023.³⁸ This limits any potential impact to only one presidential and one midterm election (and the more recently relevant gubernatorial recall).

Deepfakes have created a political problem for which there is almost no tangible solution. Part II of this Note will provide an overview of what deepfakes are, outline why they present a democratic crisis, and discuss how A.B. 730 attempts to address that crisis—for better and for worse. Part III of this Note will address the redundancy created by the law, given the existence of already efficient remedies. Part IV will analyze the constitutional hurdles A.B. 730 faces by restricting political speech. And Part V will present the challenges facing the enforcement of A.B. 730, given the burdens facing litigants and protections for internet service providers.

Although A.B. 730 is well-intentioned, the practical impacts of the law render it essentially toothless. Effective legislation against deepfakes is still needed, particularly at the federal level, but that is yet to come.

II. WHAT IS A DEEPPFAKE?

Deepfakes are manipulated images, audio, or video, designed to make the altered media seem authentic.³⁹ They can either amend the truth just slightly (by modifying an original image or video) or be

36. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

37. *See id.* The law amended Section 20010 of the California Elections Code to include a provision stating that “[t]his section shall not be construed to alter or negate any rights, obligations, or immunities of an interactive service provider under Section 230 of Title 47 of the United States Code.”

38. *Id.*

39. Chesney & Citron, *supra* note 10, at 1758 (defining deepfakes as “technology [that] . . . leverages machine-learning algorithms to insert faces and voices into video and audio recordings of actual people and enables the creation of realistic impersonations out of digital whole cloth. The end result is realistic-looking video or audio making it appear that someone said or did something.”).

forgeries outright.⁴⁰ Altered media itself is not inherently new technology (Adobe Photoshop, for example, has existed since 1987).⁴¹ Stalin was even known for having various political opponents cleverly edited out of photos, well before the dawn of the digital age.⁴² But until recently, the process of creating manipulated images or video has been “a slow, painstaking process usually reserved for experts trained in the vagaries of software like . . . Photoshop or After Effects.”⁴³

Now, the ability to manipulate media has accelerated through the advent of artificial intelligence (AI) tools, making the technology easier to use and more widely available to the public.⁴⁴ The initial development of deepfake technology was fairly rudimentary, and involved users taking “off-the-shelf AI tools to paste celebrities’ faces onto pornographic video clips.”⁴⁵ This effect was achieved through a process commonly known as “deep learning.”⁴⁶

Deep learning is a form of AI or “machine learning,” where computers learn to perform tasks that previously required human input or intelligence.⁴⁷ Deep learning builds on the basic premise of AI, by having “artificial neural networks . . . learn from large amounts of data.”⁴⁸ Neural networks are “a means of doing machine learning, in which a computer learns to perform some task by analyzing training examples.”⁴⁹ Much like humans learn from experience, neural networks perform tasks repeatedly, improving their output with every repetition.⁵⁰ Deepfakes are generated by having these deep learning algorithms study an original video clip alongside images of the face

40. *Id.*

41. *Adobe Photoshop*, ENCYC. BRITANNICA, <https://www.britannica.com/technology/Adobe-Photoshop> (last visited Apr. 11, 2021).

42. Masha Gessen, *The Photo Book that Captured How the Soviet Regime Made the Truth Disappear*, NEW YORKER (July 15, 2018), <https://www.newyorker.com/culture/photo-booth/the-photo-book-that-captured-how-the-soviet-regime-made-the-truth-disappear>.

43. Cade Metz, *Internet Companies Prepare to Fight the ‘Deepfake’ Future*, N.Y. TIMES (Nov. 24, 2019), <https://www.nytimes.com/2019/11/24/technology/tech-companies-deepfakes.html>.

44. *Id.*

45. Vincent, *supra* note 7.

46. *Id.*

47. Bernard Marr, *What Is Deep Learning AI? A Simple Guide With 8 Practical Examples*, FORBES (Oct. 1, 2018, 12:16 AM), <https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/>.

48. *Id.*

49. Larry Hardesty, *Explained: Neural Networks*, MIT NEWS (Apr. 14, 2017), <https://news.mit.edu/2017/explained-neural-networks-deep-learning-0414>.

50. Marr, *supra* note 47.

the creator wants to swap into the clip.⁵¹ In order to create a deepfake, “AI-driven software detects the way a subject moves his or her mouth and face from the source images and duplicates those movements on the subject of another video.”⁵² In effect, the computer is training itself on how to best merge the two, in order to generate a convincing dupe.⁵³

Deepfakes are beginning to progress beyond mere deep learning, which is primarily used to discriminate between varying data inputs.⁵⁴ Generative adversarial networks (GANs) are pushing the medium forward by using two different neural networks in opposition to one another.⁵⁵ One develops the deepfake, while the other (the “adversarial network”), tries to determine flaws in the quality of the clip.⁵⁶ They repeat this pattern, until the machine-generated media becomes concerningly realistic.⁵⁷ In fact, while DARPA, “the research arm of the U.S. military, is spending millions to develop tools that detect deepfakes, their technologists admit that if a creator uses Generative Adversarial Networks (GANs), their work will in most cases be able to circumvent any . . . detection software.”⁵⁸

For now, the process of developing a high quality deepfake still requires a savvy coder, a powerful computer, and some patience.⁵⁹ But the technology is improving at a rapid rate, and commercial applications are beginning to offer the ability to make certain types of face swapping content with relative ease.⁶⁰ Software programs such as “FakeApp” are available for any internet user to download, and allow them to make decent (although not seamless) deepfakes.⁶¹ This

51. Matt Binder, *Deepfakes Are Getting Easier to Make and the Internet's Just Not Ready*, MASHABLE (Jan. 17, 2020), <https://mashable.com/article/deepfake-impersonation-tech-easy-to-make>.

52. Herbert B. Dixon Jr., *Deepfakes: More Frightening Than Photoshop on Steroids*, JUDGES' J., Spring 2019, at 35, 36.

53. Binder, *supra* note 51.

54. Elizabeth Caldera, Note, “Reject the Evidence of Your Eyes and Ears”: Deepfakes and the Law of Virtual Replicants, 50 SETON HALL L. REV. 177, 181 (2019).

55. Chesney & Citron, *supra* note 10, at 1760.

56. *Id.*

57. *Id.*

58. Jared Schroeder, *Free Expression Rationales and the Problem of Deepfakes Within the E.U. and U.S. Legal Systems*, 70 SYRACUSE L. REV. 1171, 1178 (2020).

59. Binder, *supra* note 51.

60. Ivan Mehta, *New Deepfake App Pastes Your Face onto GIFs in Seconds*, THE NEXT WEB (Jan. 13, 2020), <https://thenextweb.com/artificial-intelligence/2020/01/13/new-deepfake-app-pastes-your-face-onto-gifs-in-seconds/>.

61. Matt Binder, *The U.S. Defense Department Is Ready for the Battle Against Deepfakes*, MASHABLE (Aug. 7, 2018), <https://mashable.com/article/defense-department-fighting-deepfakes>; Caldera, *supra* note 54, at 185.

software is built upon TensorFlow, Google’s “internal tool for developing artificial intelligence algorithms,” which is available to the public (and often used in its raw form by more skilled deepfake creators).⁶² Although the commercial intent of deepfakes technology is predominately for lighthearted entertainment, the vast majority of deepfakes (96 percent) have been used to create pornography.⁶³ While this usage presents its own range of legal challenges, the potential negative impacts of deepfake technology in the political sphere (as in the Pelosi video) have raised alarm nationwide, including in California.

A.B. 730 is a byproduct of legislators’ desire to manage and contain the impact of malicious deepfakes. Specifically, it is among the first pieces of legislation related to deepfakes (particularly political deepfakes) to actually become law.⁶⁴ It therefore has the ability to set both beneficial and harmful precedents for how other states (and the federal government) choose to address the burgeoning technology.

One of the most valuable sections of the law details the state’s definition of deepfakes (or what it refers to as “materially deceptive audio or visual media”). A.B. 730 defines this as:

an image or an audio or video recording of a candidate's appearance, speech, or conduct that has been intentionally manipulated in a manner such that both of the following conditions are met:

- (1) The image or audio or video recording would falsely appear to a reasonable person to be authentic.
- (2) The image or audio or video recording would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording.⁶⁵

This provides a fairly holistic definition of what a deepfake is (an “image or audio or video recording . . . that has been intentionally

62. Douglas Harris, Note, *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, 17 DUKE L. & TECH. REV. 99, 99–100 (2019).

63. Kari Paul, *California Makes ‘Deepfake’ Videos Illegal, but Law May Be Hard to Enforce*, THE GUARDIAN (Oct. 7, 2019), <https://www.theguardian.com/us-news/2019/oct/07/california-makes-deepfake-videos-illegal-but-law-may-be-hard-to-enforce>.

64. Ruiz, *supra* note 20.

65. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

manipulated . . . [to] falsely appear . . . fundamentally different”).⁶⁶ It incorporates the various types of manipulatable media, and describes the purpose, function, and impact of deepfakes in a straightforward manner. The strength of this definition is arguably A.B. 730’s best offering. By having a well-rounded and reasonable set of parameters for what constitutes a deepfake, the law provides an excellent precedent for other states or federal lawmakers to draw upon.

Beyond its definitions, A.B. 730 has already begun to make an impact, particularly in the above-board, commercial deepfakes market. In September 2020, Impressions (a cell phone app which allows users to create semi-realistic deepfakes from their phones) removed the option to create videos with the face of then-President Donald Trump, citing concerns of non-compliance with A.B. 730.⁶⁷ Other popular deepfake-creating apps, such as Reface, still allow users to swap their face onto the faces of political figures, but do not allow them to create altered videos that appear to be of the politicians themselves.⁶⁸ Another one of these apps, Avatarify, allows users to upload any photo (including of politicians), and then “control the face of [that] person like a puppet.”⁶⁹ But, legitimate apps (with formal protocols, terms and conditions, watermarks, and legal advisors) are hardly the law’s primary intended target. At its core, A.B. 730 was designed to “protect voters from being tricked and influenced by manipulated videos, audio recordings, or images before an election”—not humorous Trump impressions made by your average citizen on an iPhone.⁷⁰ The fact that the law’s only practical application thus far has been on the business practices of entertainment apps makes its failings all the more glaring. The stakes are inherently higher for deepfakes that are spread with manipulative intent.

66. *Id.*

67. Mikael Thalen, *Deepfake App Takes Trump Videos Offline Until After the Election*, DAILY DOT (Sept. 2, 2020, 2:05 PM), <https://www.dailydot.com/debug/deepfake-app-trump-2020-election>.

68. See Natasha Lomas, *Deepfake Video App Reface Is Just Getting Started on Shapeshifting Selfie Culture*, TECHCRUNCH (Aug. 17, 2020, 10:35 AM), <https://techcrunch.com/2020/08/17/deepfake-video-app-reface-is-just-getting-started-on-shapeshifting-selfie-culture>.

69. Geoffrey A. Fowler, *Anyone with an iPhone Can Now Make Deepfakes. We Aren’t Ready for What Happens Next*, WASH. POST (Mar. 25, 2021, 5:00 AM), <https://www.washingtonpost.com/technology/2021/03/25/deepfake-video-apps/>.

70. *Elections: Deceptive Audio or Visual Media*, *supra* note 15, at 6.

III. A.B. 730 IS REDUNDANT, GIVEN EXISTING STATE LAW

In modifying section 20010 of the California Elections Code, A.B. 730 sets out two possible causes of action in relation to political deepfakes.

First, any “registered voter” can file for a temporary restraining order, seeking to enjoin the “publication, distribution, or broadcasting of any campaign material” in violation of the law.⁷¹ This form of unrelated third-party claim is one of the only non-redundant portions of the statute.⁷² Second, a candidate for public office who appears in a digitally manipulated form of media can seek both injunctive relief and damages.⁷³ This type of claim is equivalent to other causes of action codified in California, such as defamation, false light, and even the right of publicity.

The ability for a private citizen (so long as they are registered to vote) to seek a temporary restraining order against a deepfake is one of the only legally innovative portions of A.B. 730. There is no requirement for this citizen to be featured in the manipulated media or have any connection to anyone featured in the media.⁷⁴ In practice, this means that anyone could file a complaint on behalf of an elected official (so long as the other requirements of the law, in terms of timing and content, are met). This opens the door to possibly endless frivolous lawsuits, which would further burden California’s already taxed court system.⁷⁵

By contrast, unrelated third parties cannot file actions for other types of reputation-oriented harm in California, such as defamation or false light.⁷⁶ Even for a tort law claim for violation of the right of publicity, outside persons can only file suit if the issue pertains to

71. Cal. Assemb. B. 730.

72. Third parties, such as relatives of a deceased person, cannot sue for defamation under California law. *See Kelly v. Johnson Publ’g Co.*, 325 P.2d 659, 662 (Cal. Ct. App. 1958) (holding that “[d]efamation of a deceased person does not give rise to a civil right of action at common law in favor of the surviving spouse, family, or relatives, who are not themselves defamed”).

73. Cal. Assemb. B. 730.

74. *See id.*

75. Micha Star Liberty, *Op-Ed: Why the State Court System Is Experiencing a Pandemic Meltdown*, L.A. TIMES (Sept. 7, 2020, 3:05 AM), <https://www.latimes.com/opinion/story/2020-09-07/courts-and-covid-hed>.

76. For defamation, see *Kelly*, 325 P.2d at 662; false light is one type of invasion of privacy tort. *See Forsher v. Bugliosi*, 608 P.2d 716, 725 (Cal. 1980). The right of privacy “cannot be asserted by anyone other than the person whose privacy is invaded.” 6A CAL. JUR. 3D *Assault and Other Willful Torts* § 143, Westlaw (database updated Feb. 2021).

postmortem publicity rights and the moving party is a legal heir or relative.⁷⁷

Putting the novelty of third party filings aside, the second cause of action (for political candidates) in A.B. 730 is functionally redundant. Defamation and false light already meet a would-be plaintiff's needs, and depending on the particulars, so too might the right of publicity. A.B. 730 could also be considered redundant in light of federal copyright law. The copyright holder of a manipulated piece of media could file a claim against a deepfake's creator (if they are able to find them), or at the very least, send a Digital Millennium Copyright Act (DMCA) takedown notice to internet service providers to stop its spread.⁷⁸ These redundancies serve to limit the impact of the law, and could possibly drive potential plaintiffs away from using it, given the more established options available.

A. A.B. 730 Is Redundant Under California's Defamation Statutes

California's Civil Code provides a cause action for defamation, which is defined as "a false and unprivileged publication that exposes the plaintiff 'to hatred, contempt, ridicule, or obloquy, or which causes him to be shunned or avoided, or which has a tendency to injure him in his occupation.'" ⁷⁹ Defamation is effected by way of either libel (defamation in written form) or slander (oral defamation).⁸⁰ For public figures, defamation requires a showing of actual malice—"knowledge that [the statement] was false or with reckless disregard of whether it was false."⁸¹ Similar to the false publication requirement for defamation, A.B. 730 requires the publication or distribution of campaign material that "create[s] a false representation."⁸² And because A.B. 730 also concerns the reputations of public figures, it too

77. CAL. CIV. CODE § 3344.1 (Deering 2021).

78. A DMCA takedown occurs "[w]hen content is removed from a website at the request of the owner of the content or the owner of the copyright of the content. It is a well established, accepted, internet standard followed by website owners and internet service providers." *What is a DMCA Takedown?*, DMCA.COM, <https://www.dmca.com/FAQ/What-is-a-DMCA-Takedown> (last visited Apr. 11, 2021).

79. *Brodeur v. Atlas Ent., Inc.*, 204 Cal. Rptr. 3d 483, 492 (Ct. App. 2016) (citations omitted).

80. See CAL. CIV. CODE §§ 44, 45(a), 46.

81. *Dickinson v. Cosby*, 250 Cal. Rptr. 3d 350, 364 (Ct. App. 2019); see also *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 279–81 (1964) (stating that a public official cannot recover "for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice'—that is, with knowledge that it was false or with reckless disregard of whether it was false or not").

82. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

requires a demonstration of actual malice, which is defined by the statute to mean “the knowledge that the image of a person has been superimposed on a picture or photograph to create a false representation, or a reckless disregard of whether or not the image of a person has been superimposed on a picture or photograph to create a false representation.”⁸³

Another important similarity between the causes of action is believability. A defamation case can turn on whether the statement in question is believable as fact or clearly a joke.⁸⁴ For example, “a speech made after dinner, understood by all present as a harmless joke, may amount to libel when it is published in a newspaper and reaches those who do not understand the circumstances.”⁸⁵ Comparably, A.B. 730 requires the “materially deceptive audio or visual media” to “cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording.”⁸⁶

In light of the similar requirements, a candidate for public office could more easily use existing defamation law to seek either injunctive relief or damages, given the wide body of caselaw which litigants can already turn to for support. This overlap is additionally relevant given the time limitation contained in A.B. 730—the material in question must be distributed within sixty days of an election.⁸⁷ This means that if the material were distributed sixty-one days before an election, A.B. 730 would not apply (but defamation law would). Using traditional defamation law would instead allow a plaintiff greater flexibility, while achieving the same type of outcomes (removal of the deepfake, financial compensation, etc.).

B. A.B. 730 Is Redundant, Given California’s Existing Body of “False Light” Law

Even if a litigant could not meet the standards required for defamation, A.B. 730 is still redundant given the invasion of privacy

83. *Id.*

84. *Hustler Mag., Inc. v. Falwell*, 485 U.S. 46, 52–54 (1988); *Arno v. Stewart*, 54 Cal. Rptr. 392, 396 (Ct. App. 1966).

85. *Arno*, 54 Cal. Rptr. at 397.

86. Cal. Assemb. B. 730.

87. *Id.*

tort of false light. The elements needed for this claim are “a portrayal of the plaintiff which casts him or her in a false light and that is objectionable to a reasonable person, and publication of the portrayal.”⁸⁸ The distinction between false light and defamation is that the “plaintiff is not required to prove that the defendant knowingly directed the portrayal at him or her.”⁸⁹ In effect, this makes it *easier* to state a claim for false light than it does to make a claim under A.B. 730, because there is neither an intent standard nor election timing to consider. Casting in a false light is parallel to the “false representation” requirement of A.B. 730, as are the reasonable person and publication requirements. Again, although some of the elements of the two laws are similar, the substantially easier (and likely more fruitful) course of action would be for a litigant to file a false light claim because of the greater volume of precedent and decreased burden.

C. A.B. 730 May Be Redundant Under California Right of Publicity Law

California boasts some of the most robust and comprehensive right of publicity laws in the United States.⁹⁰ The right of publicity is defined as “the inherent right of every human being to control the commercial use of his or her identity.”⁹¹ Among California’s right of publicity laws is section 3344 of the California Civil Code, which provides a cause of action for “knowingly us[ing] another’s name, voice, signature, photograph, or likeness, in any manner . . . without such person’s prior consent.”⁹² This statute would allow a candidate for public office to file a claim for the nonconsensual use of their voice, photograph, or likeness in a deepfake if that deepfake was being used for commercial purposes or in advertisements.⁹³ This again mirrors A.B. 730, which prohibits deepfakes in campaign materials specifically. The law explicitly defines “campaign materials” to

88. CAL. CIV. PRAC. TORTS *Common Law Action* § 20:12, Westlaw (database updated Nov. 2020).

89. *Id.*

90. Jennifer Rothman, *California*, ROTHMAN’S ROADMAP TO THE RIGHT OF PUBLICITY (updated Aug. 16, 2019), <https://www.rightofpublicityroadmap.com/law/california>.

91. 1 J. THOMAS MCCARTHY & ROGER E. SCHECHTER, RIGHTS OF PUBLICITY AND PRIVACY 2D § 1:3, Westlaw (database updated May 2020).

92. CAL. CIV. CODE. § 3344 (Deering 2021).

93. *Id.*

include “advertisement[s] in a newspaper or other periodical, television commercial, or computer image.”⁹⁴

However, a right of publicity claim also requires an unapproved user to be exploiting the plaintiff’s identity for financial gain.⁹⁵ This does not necessarily bar deepfakes from falling under the auspices of right of publicity law, but it does make it significantly more unlikely in the political sphere. It would be extraordinarily challenging to prove perpetrators, who are nearly impossible to locate in the first place, were directly profiting off the proliferation of a political deepfake. This is in part because “the harms associated with deep fakes do not typically generate direct financial gain for their creators.”⁹⁶ Even if the perpetrator were to be, for example, an opposing campaign, this would still not necessarily mean they were receiving a commercial (as opposed to political) benefit from the spread of the deepfake. That being said, if an opposing campaign were to use a deepfake of unknown origin in their advertising (without previously determining its veracity), the candidate featured could have a viable right of publicity claim against them (without being bogged down by the timing and intent constraints of A.B. 730).

Although this overlap is more limited, it once again demonstrates the redundancies between A.B. 730 and existing law.

D. A.B. 730 Is Redundant Under the Digital Millennium Copyright Act

Not all deepfakes are original works—many exploit already existing, copyrighted content.⁹⁷ For deepfake victims, this “open[s] the door to monetary damages and a notice-and-takedown procedure that can result in removal of the offending content.”⁹⁸

Deepfakes that contain copyrighted material would fall under the purview of the DMCA.⁹⁹ The DMCA is a federal statute which grants protections to copyright owners whose media is being illegally proliferated online.¹⁰⁰

94. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

95. Chesney & Citron, *supra* note 10, at 1794.

96. *Id.*

97. *Id.* at 1793.

98. *Id.*

99. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

100. *Id.*

The statute contains “anti-circumvention” provisions, which allow for the removal or “takedown” of copyrighted material spread by nonowners.¹⁰¹ If a copyright holder discovers their media online, they can send a DMCA takedown notice “to a service provider requesting the provider to remove material that is infringing their copyright[.]”¹⁰² A service provider can mean a true internet service provider (like Comcast or Spectrum), or a general website, search engine, or social media network (like Google or YouTube).¹⁰³

DMCA takedown notices are not limited to copyright holders alone: “a takedown request can be made by anyone who is the subject of a video—a provision arguably broad enough to include all deepfake victims.”¹⁰⁴ Because of this provision, a victim of a political deepfake (regardless of whether they own the copyright to the video) would likely be able to remove their media from the internet by issuing a takedown notice.¹⁰⁵ Simplifying matters further, a formal copyright registration is not required to issue a DMCA takedown notice.¹⁰⁶

This would be a far easier path for a victim than utilizing A.B. 730. They would only have to demonstrate their presence in the video or their copyright ownership, as opposed to locating the perpetrator, establishing “actual malice,” etc. This also allows for a more immediate and efficient response to a political deepfake, especially if the victim’s first concern is getting the media away from vulnerable eyes.

Of course, this method is not foolproof. Whoever posted the video (if they are willing to come forward) can file a counter-notice,¹⁰⁷ and

101. *Digital Millennium Copyright Act*, ELEC. FRONTIER FOUND., <https://www.eff.org/issues/dmca> (last visited Apr. 11, 2021).

102. *What Is the DMCA Notice and Takedown Process?*, COPYRIGHT ALL., https://copyrightalliance.org/ca_faq_post/dmca-notice-and-takedown-process (last visited Apr. 11, 2021).

103. *Id.*

104. Delfino, *supra* note 5, at 936.

105. Although this strategy could come up against fair use arguments by the creators of the altered media, they would have to come forward in order to make this assertion, which is unlikely given the highly anonymous nature of deepfakes creation. Additionally, the inherently malicious nature of political deepfakes would likely undermine any legitimate fair use claim.

106. *See What Is the DMCA Notice and Takedown Process?*, *supra* note 102.

107. If an alleged infringer believes, in good faith, that his or her activity is not infringing, he or she can send a “counter notice to the service provider explaining why they disagree with the copyright owner. Like the takedown notice, there are certain elements that must be contained in a DMCA counter notice.” *DMCA Counter-Notice Process*, COPYRIGHT ALL., <https://copyrightalliance.org/education/copyright-law-explained/the-digital-millennium-copyright-act-dmca/dmca-counter-notice-process/> (last visited Mar. 18, 2021).

not every copy of the media may be able to be tracked down and removed. But this still demonstrates yet another possible alternative cause of action available to litigants, with fewer limitations than A.B. 730.

Redundancy in-and-of-itself is not necessarily problematic. But A.B. 730 contains greater flaws than mere repetition.

IV. A.B. 730 PLACES POTENTIALLY UNCONSTITUTIONAL LIMITATIONS ON FREEDOM OF SPEECH

In general, “the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content.”¹⁰⁸ Because A.B. 730 explicitly codifies a form of expression-based restriction, it would be unlikely to withstand a constitutional challenge on First Amendment grounds. Although the constitutionality of the law has yet to be tested, possible challenges abound.¹⁰⁹ This is primarily because laws curtailing speech based on its “communicative content . . . are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests.”¹¹⁰

Manipulated media—whether in image, audio, and video form—is inherently communicative content, protected by the First Amendment.¹¹¹ Deepfakes specifically can communicate messages on topics ranging from humorous to pornographic to political. The communicative nature of deepfakes makes them generally protectable by the First Amendment, which is incorporated against the states via the Fourteenth Amendment (meaning it applies to California state laws).¹¹² The curtailing of deepfakes outlined by A.B. 730 is explicitly dependent on their content. Deepfakes on the whole, are not prohibited

108. *Ashcroft v. Am. Civ. Liberties Union*, 535 U.S. 564, 573 (2002) (quoting *Boulger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 65 (1983)).

109. As of May 1, 2021.

110. *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015) (first citing *R.A.V. v. City of St. Paul*, 505 U.S. 377, 395 (1992)); and then citing *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105, 115, 118 (1991)).

111. See Charlotte Stanton et al., *The Legal, Ethical, and Efficacy Dimensions of Managing Synthetic and Manipulated Media*, CARNEGIE ENDOWMENT FOR INT’L PEACE (Nov. 15, 2019), <https://carnegieendowment.org/2019/11/15/legal-ethical-and-efficacy-dimensions-of-managing-synthetic-and-manipulated-media-pub-80439> (“An outright legal ban on synthetic and manipulated media would violate the First Amendment because ‘falsity alone’ does not remove expression from First Amendment protection, and many digital falsifications would be constitutionally protected speech.”).

112. *Reed*, 576 U.S. at 163.

by the law—rather only campaign materials that “contain[] (1) a picture or photograph of a person or persons into which the image of a candidate for public office is superimposed or (2) a picture or photograph of a candidate for public office into which the image of another person or persons is superimposed.”¹¹³ This means A.B. 730 governs not just political speech, but also false speech. Because A.B. 730 is explicitly “content based,” this:

requires a court to consider whether a regulation of speech ‘on its face’ draws distinctions based on the message a speaker conveys. . . . Some facial distinctions based on a message are obvious, defining regulated speech by particular subject matter, and others are more subtle, defining regulated speech by its function or purpose. Both are distinctions drawn based on the message a speaker conveys, and, therefore, are subject to strict scrutiny.¹¹⁴

Restrictions against content-based speech, and political speech in particular, are held to the highest standard of judicial oversight—strict scrutiny.¹¹⁵ Thus, “[a] law that is content based on its face is subject to strict scrutiny regardless of the government’s benign motive, content-neutral justification, or lack of ‘animus toward the ideas contained’ in the regulated speech.”¹¹⁶ Strict scrutiny is required whenever the government proposes a law which may impinge on a fundamental freedom or interest.¹¹⁷ Therefore, “[c]ontent-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only [by meeting the criteria of strict scrutiny].”¹¹⁸ In order to survive a strict scrutiny analysis, the government must demonstrate that the law furthers a “compelling government interest” and is “narrowly tailored.”¹¹⁹

A.B. 730 would present a particular challenge for the government, in terms of meeting the standards required for strict scrutiny. This is because the law is not only focused on political

113. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

114. *Reed*, 576 U.S. at 163–64 (internal citations omitted).

115. 13 CAL. JUR. 3D *Constitutional Law* § 254, Westlaw (database updated Feb. 2021).

116. *Reed*, 576 U.S. at 165 (quoting *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 429 (1993)).

117. *Id.* at 163.

118. *Id.*

119. *Citizens United v. Fed. Election Comm’n*, 558 U.S. 310, 340 (2010).

speech, but rather a subset of it: campaign speech. As *Citizens United v. Federal Election Commission*¹²⁰ explains, “[t]he First Amendment “has its fullest and most urgent application” to speech uttered during a campaign for political office.”¹²¹

A. A.B. 730 Does Not Further a “Compelling Government Interest”

Defining a “compelling government interest” is easier said than done. The Supreme Court has never provided clear guidelines as to what makes a government interest compelling or not.¹²² Interests that have been defined as “compelling” include national security,¹²³ “allowing governmental entities to perform their functions,”¹²⁴ and maintaining a stable political system.¹²⁵

In the context of A.B. 730, the government could propose a number of state interests to justify the law, including political stability, the regulation of elections, and stopping the spread of misinformation. Many of these were in fact raised by the California State Senate in its Committee on Elections and Constitutional Amendments’ digest on the proposed law.¹²⁶ However, any of those interests would be mitigated by a series of Supreme Court cases which undermine the government’s ability to regulate electoral speech—even if it is false.

For example, in *Brown v. Hartlage*,¹²⁷ the Supreme Court held that in relation to a Kentucky election regulation, “preserving the integrity of [the] electoral process[.]” was only a “legitimate” state interest, and not a “compelling” one.¹²⁸ Specifically, “fear that voters might make an ill-advised choice does not provide the State with a compelling justification for limiting speech. It is simply not the function of government to ‘select which issues are worth discussing or

120. 558 U.S. 310 (2010).

121. *Id.* at 339 (quoting *Eu v. S.F. Cnty. Democratic Cent. Comm.*, 489 U.S. 214, 223 (1989)).

122. Robert T. Miller, *What Is a Compelling Governmental Interest?* 1 (Univ. of Iowa Legal Stud. Rsch. Paper No. 2018-1, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=314916

2.

123. *See Korematsu v. United States*, 323 U.S. 214, 225 (1944).

124. *Citizens United*, 558 U.S. at 341.

125. *Storer v. Brown*, 415 U.S. 724, 736 (1974).

126. *See generally Elections: Deceptive Audio or Visual Media: Hearing on Assembly Bill No. 730 Before the S. Comm. on the Judiciary*, 2019–2020 Reg. Sess. 6–7 (Cal. 2019) (as amended June 25, 2019) (stating that many authors and opponents of the bill agree that election integrity constitutes a compelling government interest).

127. 456 U.S. 45 (1982).

128. *Id.* at 52–54.

debating.”¹²⁹ Based on this precedent, regulating altered media, even if that media could manipulate voters into making an “ill-advised choice,” would not satisfy a compelling government purpose.

Moreover, in *Susan B. Anthony List v. Driehaus*,¹³⁰ the Supreme Court struck down Ohio state laws that prohibited “certain false statement[s] during the course of any campaign for nomination or election to public office or office of a political party.”¹³¹ The facts of that case prove particularly relevant to A.B. 730. Susan B. Anthony List is an anti-abortion organization, which published a press release asserting that the then recently-passed Affordable Care Act would authorize “taxpayer-funded abortion.”¹³² In the statement, the organization included the name of an Ohio Congressman after he voted in favor of the Act.¹³³ The Congressman filed a complaint after the release damaged his reelection campaign.¹³⁴ The Ohio Elections Commission determined that the claim regarding government funded abortions was false, and therefore that the organization violated the statute (after the Congressman withdrew his complaint, the District court lifted the stay and Susan B. Anthony List amended its complaint asserting the statutes were unconstitutional by chilling speech).¹³⁵ Due to this dispute, the Court found that “the ‘practical effect’ of the Ohio false statement scheme is ‘to permit a private complainant . . . to gain a campaign advantage without ever having to prove the falsity of a statement.’”¹³⁶ The Court reasoned that silencing Susan B. Anthony List’s speech, even if that speech was potentially false, was unconstitutional and could create electoral unfairness towards other, non-targeted candidates.¹³⁷

In contrast to preventing false speech, the Supreme Court *has* held that “maintaining a stable political system” qualifies as a compelling government interest.¹³⁸ California could argue that in curbing the spread of misinformation via deepfakes, A.B. 730 is doing just that. But, following the logic used by the Court in *Eu v. San Francisco*

129. *Id.* at 60.

130. 573 U.S. 149 (2014).

131. *Id.* at 152–53 (internal quotations omitted).

132. *Id.* at 153–54.

133. *Id.* at 154.

134. *Id.*

135. *Id.* at 162–63.

136. *Id.* at 165 (omission in original).

137. *Id.* at 164–66.

138. *Eu v. S.F. Cnty. Democratic Cent. Comm.*, 489 U.S. 214, 226 (1989).

County Democratic Central Committee,¹³⁹ California would have to demonstrate *how* this law directly improved the stability of the state’s political system.¹⁴⁰ Moreover, the Court asked the state of California then—and any court would presumably ask the state now—“what makes the California system so peculiar that it is virtually the only State that has determined that such a ban is necessary”?¹⁴¹ In this case, other states have implemented similar laws (namely Texas, with Senate Bill 751),¹⁴² but this type of policy specifically targeting political deepfakes is hardly widespread.¹⁴³ Even if this interest was compelling, a court would still have to assess whether the rationale was *compelling enough* to justify the rather heavy burden A.B. 730 places on free speech.¹⁴⁴ Critiquing candidates is one of the most central tenets of election discourse, and not all forms of manipulated media involving valid candidate critiques would necessarily fall within the exceptions outlined by A.B. 730 (such as satire or parody).¹⁴⁵

Aside from whether the state developed its own compelling interest, there are certain types of free speech restrictions the Supreme Court *has* upheld. Namely, “content-based restrictions on speech have been permitted, as a general matter, only when confined to the few ‘historic and traditional categories [of expression] long familiar to the bar.’”¹⁴⁶ These categories include incitement of violence, obscenity, fraud, defamation of private citizens, “speech integral to criminal conduct,” and child pornography, among others.¹⁴⁷ Political deepfakes generally do not fall into any of these categories.

B. A.B. 730 Is Not “Narrowly Tailored”

Once a state has articulated how a law in question furthers a “compelling government interest,” the next requirement of strict

139. 489 U.S. 214 (1989).

140. *Id.* at 226.

141. *Id.*

142. S.B. 751, 86th Leg. (Tex. 2019).

143. Carolyn Toto & Taylor Keating, *Protecting Elections: Regulating Deepfakes in Politics*, JD SUPRA (Aug. 7, 2020), <https://www.jdsupra.com/legalnews/protecting-elections-regulating-39567>. Unlike in California, there has already been some activity related to Texas Senate Bill 751. Houston Mayor Sylvester Turner asked the city’s district attorney to investigate his political opponents use of edited text messages and photos of him in a television campaign ad. *Id.*

144. *See Eu*, 489 U.S. at 222.

145. *See Assemb. B. 730*, 2019–2020 Reg. Sess. (Cal. 2019).

146. *United States v. Alvarez*, 567 U.S. 709, 717 (2012) (alteration in original).

147. *Id.*

scrutiny is that the law be “narrowly tailored” to meet that purpose.¹⁴⁸ For a law restricting content-based speech to be “narrowly tailored,” it must not “burden substantially more speech than is necessary to further the government's legitimate interests.”¹⁴⁹ Moreover, the government must show that “alternative measures that burden substantially less speech would fail to achieve the government's interests, not simply that the chosen route is easier.”¹⁵⁰ This requirement forces the government to avoid silencing speech for mere convenience, and “prevents the government from too readily ‘sacrific[ing] speech for efficiency.’”¹⁵¹

A.B. 730 substantially burdens electoral speech by eliminating all legitimate uses for manipulated videos involving candidates for public office, unless those videos fall into a few narrow exceptions (such as parody or satire).¹⁵² It limits valid critiques of candidates which could occur through the medium without necessarily being “funny.” Moreover, A.B. 730 could “prohibit the use of altered content to reenact true events that were not recorded or could bar a candidate’s use of their own altered videos” in counter-attack ads.¹⁵³

Several of the political groups which opposed A.B. 730, including the American Civil Liberties Union (ACLU) and California Newspaper Publishers Association (CNPA), were quick to draw comparisons between A.B. 730 and the Ohio statutes in *Susan B. Anthony List*.¹⁵⁴ After that case was remanded by the Supreme Court, it was once again reviewed by the Sixth Circuit. In their subsequent holding, the Sixth Circuit pointed out that the Ohio laws were overturned “because they [were] not narrowly tailored in their (1) timing, (2) lack of a screening process for frivolous complaints, (3) application to non-material statements, (4) application to commercial intermediaries, and (5) over-inclusiveness and under-inclusiveness.”¹⁵⁵ Both the ACLU and CNPA argued that these issues

148. *McCullen v. Coakley*, 573 U.S. 464, 477 (2014).

149. *Id.* at 486 (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989)).

150. *Id.* at 495.

151. *Id.* at 486 (alteration in original) (quoting *Riley v. Nat’l Fed’n of the Blind of N.C., Inc.*, 487 U.S. 781, 795 (1988)).

152. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

153. David E. Fink & Sarah E. Diamond, *Deepfakes: 2020 and Beyond*, THE RECORDER (Sept. 3, 2020), <https://www.law.com/therecorder/2020/09/03/deepfakes-2020-and-beyond>.

154. *Elections: Deceptive Audio or Visual Media: Hearing on Assembly Bill No. 730 Before the S. Comm. on the Judiciary*, *supra* note 126, at 7.

155. *Susan B. Anthony List v. Driehaus*, 814 F.3d 466, 474 (6th Cir. 2016).

were equally applicable to A.B. 730 (particularly because it was overbroad).¹⁵⁶

The most directly comparable issue between the two laws is their timing. The Ohio law posed issues because “there [was] no guarantee the administrative or criminal proceedings [would] conclude before the election or within time for the candidate’s campaign to recover from any false information that was disseminated.”¹⁵⁷ This meant that decisions regarding the outcome of any electoral damage would be made post-election, when it was too late to have an impact.¹⁵⁸ Similarly, with A.B. 730, the law bars the distribution of deepfakes “within 60 days of an election.”¹⁵⁹ This leaves very little time for effective adjudication before an election would actually take place, even if best-case scenario, a deepfake was disseminated the full sixty days in advance.

In terms of overbreadth, California’s State Senate acknowledged the ACLU and CNPA’s concerns in their Senate Judiciary Committee Report on the initial bill.¹⁶⁰ Ultimately, they narrowed the breadth of the bill slightly by swapping the original intent standard of the law (“knowing or reckless”) for a more stringent one (“actual malice”).¹⁶¹ This decision was logical in light of *New York Times Co. v. Sullivan*,¹⁶² which established public figures must demonstrate “actual malice” in order to sue for defamation (and political candidates are inherently public figures).¹⁶³ The Committee also debated narrowing the bill by removing the ability for any registered voter to bring suit, so as to

156. *Elections: Deceptive Audio or Visual Media: Hearing on Assembly Bill No. 730 Before the S. Comm. on the Judiciary*, *supra* note 126.

157. *Susan B. Anthony List*, 814 F.3d at 474.

158. *Id.*

159. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

160. *Elections: Deceptive Audio or Visual Media: Hearing on Assembly Bill No. 730 Before the S. Comm. on the Judiciary*, *supra* note 126, at 7.

161. *Id.* at 8.

162. 376 U.S. 254 (1964).

163. *Id.* at 279–80. The Court cited a Kansas Supreme Court decision as part of the rationale for this requirement, which noted that

[i]t is of the utmost consequence that the people should discuss the character and qualifications of candidates for their suffrages. The importance to the state and to society of such discussions is so vast, and the advantages derived are so great, that they more than counterbalance the inconvenience of private persons whose conduct may be involved, and occasional injury to the reputations of individuals must yield to the public welfare, although at times such injury may be great. The public benefit from publicity is so great, and the chance of injury to private character so small, that such discussion must be privileged.

Id. at 281.

diminish the risk of frivolous complaints, but ultimately decided against doing so.¹⁶⁴

Moreover, the government could find a slew of alternative approaches which would burden less speech and ultimately achieve the same ends. One approach would even be to simply amend existing defamation statutes to incorporate manipulated media targeted at candidates for office, and then apply traditional defamation requirements to political deepfakes.

Previously, the Supreme Court has not hesitated to overturn state statutes which are overbroad in their speech restrictions (especially as applied to technology). For example, in *Packingham v. North Carolina*,¹⁶⁵ the Court assessed a North Carolina law that prohibited registered sex offenders from using social media.¹⁶⁶ The Court held that although the law intended to protect children by banning sex offenders from social media outright, its practical application excessively burdened their First Amendment rights.¹⁶⁷ An inability to use social media meant barring them from access to current events, job offerings, educational resources, and more, and prevented them “from engaging in the legitimate exercise of First Amendment rights.”¹⁶⁸

Similarly here, A.B. 730 is overbroad in its restriction on deepfakes as a form of expression. Although the intent is to protect candidates from malicious content, in practice, the law would bar all deepfakes that feature their likeness. Like in *Packingham*, this results in an overbroad restriction on speech itself, unless that speech falls under one of A.B. 730’s exceptions (such as parody or adding a disclaimer to the deepfake). And while the legitimate uses for political deepfakes outside the exceptions may be few—namely artistic expression or political critique—these remain valid, protected forms of speech.

Furthermore, the state also does not narrowly tailor who can sue. Victims—namely, political candidates—are not the only people who can file a cause of action under this statute.¹⁶⁹ Any registered voter can

164. *Elections: Deceptive Audio or Visual Media: Hearing on Assembly Bill No. 730 Before the S. Comm. on the Judiciary*, *supra* note 126, at 8.

165. 137 S. Ct. 1730 (2017).

166. *Id.* at 1733.

167. *Id.* at 1737.

168. *Id.*

169. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

take umbrage, meaning the “victims” themselves do not even have to take issue with the speech in order for it to be censored. This issue of “frivolous complaints” was a problem in *Susan B. Anthony List*, and was repeatedly raised to the California Senate Judiciary Committee, to no avail.¹⁷⁰

C. Anonymous Speech is Also Protected by the First Amendment

A.B. 730 relies on the assumption that the creators of the deepfakes can and will be located, and ultimately held accountable for the media they create. The unrealistic nature of this premise is discussed in Section V below.

However, this premise also confronts another subsidiary First Amendment right—the protection of anonymous speech. The United States Supreme Court has long protected and valued anonymous speech, noting that it has “played an important role in the progress of mankind.”¹⁷¹ The Court particularly emphasized the fact that anonymous speech allows for safe criticism of oppressive leaders, laws, and policies.¹⁷²

The right to anonymously speak has serious implications in the political sphere. Fear of retaliation, or unpopularity of ideas (or their speakers) can severely hamper political speech.¹⁷³ In fact, “even in the field of political rhetoric, where ‘the identity of the speaker is an important component of many attempts to persuade,’ the most effective advocates have sometimes opted for anonymity.”¹⁷⁴ The Federalist Papers themselves provide a great example of this, given their originally anonymous nature.¹⁷⁵

The majority of deepfakes are anonymous by nature, which grants them a certain gravitas and protection. The ideas contained within political deepfakes may be either false or fringe, but that does not diminish their protected right to be expressed.

170. *Susan B. Anthony List v. Driehaus*, 814 F.3d 466, 474 (6th Cir. 2016); *Elections: Deceptive Audio or Visual Media: Hearing on Assembly Bill No. 730 Before the S. Comm. on the Judiciary*, *supra* note 126, at 7.

171. *Talley v. California*, 362 U.S. 60, 64 (1960).

172. *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 342 (1995).

173. *Id.* at 342–43.

174. *Id.* (internal citations omitted).

175. *Id.* at 342.

V. CHALLENGES OF ENFORCING INTERNET CRIMES

Putting aside questions of redundancy and constitutionality, perhaps the most pressing problem with A.B. 730 is that it is borderline impossible to implement. First, any lawsuit related to deepfakes must overcome the hurdle of actually determining a perpetrator.¹⁷⁶ Internet crimes are notoriously challenging to prosecute, given their anonymous nature, and deepfakes all the more so.¹⁷⁷ Unlike revenge porn deepfakes, where there is a smaller pool of possible suspects (given the traditionally limited initial sharing of intimate photos or videos), political deepfakes could be sourced from a wide variety of publicly available media. Political deepfakes are easily created by strangers, political operatives, or foreign nationals—all of whom may be using advanced software to hide any trail of the manipulated media's origin.¹⁷⁸

Another enforcement issue relates to the burden of proof imposed by A.B. 730's intent standard. Even if a prospective litigant *can* locate the creator of a malicious deepfake, they still have the burden of showing that creator acted with "actual malice."¹⁷⁹ Although selecting this intent standard was a sound choice by lawmakers trying to ward off constitutional challenges, it inadvertently created a substantial evidentiary burden for victims. Finally, and perhaps most crucially, A.B. 730 pointlessly places the responsibility solely on individual deepfake creators, rather than the social media platforms that spread and amplify their creations.¹⁸⁰ A malicious political deepfake, without a mechanism for widespread sharing, can only go so far. Without social media's ability to transmit deepfakes (and other forms of misinformation) without warnings or fact checking, they would have little impact. Despite this, Section 230 of the Communications Decency Act all but exempts these platforms from any liability for their spread, meaning litigants' only real recourse is to find a deepfake's specific creator.¹⁸¹

176. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

177. Matt Reynolds, *Courts and Lawyers Struggle with Growing Prevalence of Deepfakes*, ABA J. (June 9, 2020, 9:29 AM), <https://www.abajournal.com/web/article/courts-and-lawyers-struggle-with-growing-prevalence-of-deepfakes>.

178. Chesney & Citron, *supra* note 10, at 1804.

179. Cal. Assemb. B. 730.

180. *Id.*

181. *Section 230 of the Communications Decency Act*, ELEC. FRONTIER FOUND., <https://www.eff.org/issues/cda230> (last visited Apr. 11, 2021).

A. Locating Perpetrators Presents Factual and Logistical Challenges

Internet crimes are often successful because they can be executed anonymously. There is a myriad of ways to become anonymous online, both for technological novices and experts alike. There are more elementary methods, such as changing your email, going by a false name, or using a private browser.¹⁸² More advanced methods involve using proxy servers or virtual private networks (VPNs) to hide IP addresses (which link certain devices to their owners or locations).¹⁸³ In particular, the software Tor is known for its ability to mask users' identities, making it a favorite among criminals and privacy advocates alike.¹⁸⁴ When using proxy servers, VPNs, or other similar technology, "the IP addresses connected to posts may be impossible to find and trace back to the responsible parties."¹⁸⁵ As such, plaintiffs or law enforcement officials may be completely unable to track down who created the deepfake at all. Furthermore, in terms of proliferating the deepfake, many social media sites—such as Reddit and Twitter—nominally allow anonymous use.¹⁸⁶ This adds further challenges to tracing the original malicious distributor of a deepfake.

In terms of electoral deepfakes, many of the parties who have the greatest incentive to create such media are foreign powers or entities.¹⁸⁷ This too creates an additional enforcement challenge:

[t]he most capable actors with motive and means to deploy deep fakes in a high-impact manner in an election setting will include the intelligence services of foreign governments engaging in such activity as a form of covert action, as we saw with Russia in relation to the American election of 2016. The prospect of a criminal prosecution in the United States will mean little to foreign government agents involved in such activity.¹⁸⁸

182. Deb Shinder, *Online Anonymity: Balancing the Needs to Protect Privacy and Prevent Cybercrime*, TECHREPUBLIC (Sept. 20, 2011, 2:00 AM), <https://www.techrepublic.com/blog/it-security/online-anonymity-balancing-the-needs-to-protect-privacy-and-prevent-cybercrime>.

183. Dan Rafter, *Proxy vs. VPN: 4 Differences You Should Know*, NORTONLIFELOCK, <https://us.norton.com/internetsecurity-privacy-proxy-vs-vpn.html> (last visited Apr. 11, 2021).

184. Chesney & Citron, *supra* note 10, at 1792.

185. *Id.*

186. Delfino, *supra* note 5, at 899.

187. Chesney & Citron, *supra* note 10, at 1804.

188. *Id.*

A.B. 730 can thereby have little impact on some of the most effective sources of political deepfake creation.

B. Litigants Will Struggle to Meet A.B. 730's Burden of Proof

Another significant barrier to enforcement is A.B. 730's intent standard. The law requires the deepfake to have been distributed with "actual malice."¹⁸⁹ It defines "actual malice" to mean "the knowledge that the image of a person has been superimposed on a picture or photograph to create a false representation, or a reckless disregard of whether or not the image of a person has been superimposed on a picture or photograph to create a false representation."¹⁹⁰ For a party to be held liable under A.B. 730, they have to not only know what they are spreading is false, but recklessly disregard that fact (and its implications). This means that the millions of people who repost or re-share a widely proliferated deepfake across social networking sites would not be held liable for distributing the deepfake. So, while the deepfake can be shared millions of times by gullible social media users, without finding the original poster there is no cause of action.

This standard—although appropriately narrowed from a free speech perspective—creates an extraordinary burden for plaintiffs seeking to pursue litigation under A.B. 730. Finding the original distributor is a challenge enough, on top of trying to discover evidence which points to actual malice. Even if litigants or law enforcement *could* track down the origin of the deepfake, they would still face numerous logistical hurdles proving intent in a court of law.

C. A.B. 730's Pointless Disclaimers May Allow for Greater Spread of Misinformation

A.B. 730 does provide some exceptions for the dissemination of manipulated media. Specifically, the law carves out an exemption for the use of a specific disclaimer.¹⁹¹ Manipulated media accompanied by the statement, "This _____ has been manipulated," is allowed (the blank can be filled with either "image," "video," or "audio").¹⁹² The

189. Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019).

190. *Id.*

191. *Id.*

192. *Id.*

law further outlines the size the disclaimer must be, along with a series of other logistical requirements.¹⁹³

This requirement is unlikely to mean anything to malicious creators and is even ripe for abuse. Actors who are developing deepfakes with the intent to damage political candidates are not going to label their content as manipulated because it undermines the entire point of their actions. Even worse, this disclaimer could be used by malicious distributors to their advantage. For example, if a deepfakes creator released the original, unaltered form of a video with the manipulated disclaimer, and the manipulated version without it, this would inevitably sow confusion among media consumers.¹⁹⁴ This “[c]reates a false expectation that voters can trust images and videos unless they are labeled as manipulated, when in fact the bill only applies to a fraction of the misleading images and recordings that could influence an election.”¹⁹⁵ While the disclaimer is meant to allow free speech while curtailing disinformation, the process is ripe for manipulation and abuse, rendering the disclaimer pointless.

D. A.B. 730 Misplaces Responsibility for the Spread of Deepfakes by Carving Out Section 230 Immunity

A final enforcement problem for A.B. 730 derives from who it chooses to blame. The law pins responsibility for the dissemination of deepfakes on individual bad actors, rather than on the platforms who facilitate the dissemination itself. The law “shall not be construed to alter or negate any rights, obligations, or immunities of an interactive service provider under Section 230 of Title 47 of the United States Code.”¹⁹⁶ Section 230 of Title 47, better known as the Communications Decency Act (CDA) states that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”¹⁹⁷ Courts have repeatedly held that this means that online platforms are not liable for “user-generated content even if they

193. *Id.*

194. Letter from Am. Civ. Liberties Union of Cal. et al., to Members of the Cal. State Senate (Aug. 22, 2019), <https://www.eff.org/document/ab-730-berman-oppose-coalition-floor-alert-82019>.

195. *Id.*

196. Cal. Assemb. B. 730.

197. 47 U.S.C. § 230(e)(1) (2018).

deliberately encouraged the posting of that content.”¹⁹⁸ Accordingly, these same platforms cannot be held liable under A.B. 730.

Although Section 230 is considered by many to be one of the strongest forces protecting free speech online, its practical application prevents online service providers—including social media platforms—from being liable for what their users do, no matter how criminal.¹⁹⁹ This is particularly alarming in the context of deepfakes. Because users routinely share genuine news information across social media platforms, this makes it easier for false information to slip in unnoticed, among other legitimate sites.²⁰⁰ Many consumers are not savvy enough to tell the difference. Because manipulated media can be shared across the globe instantaneously via social networking sites, the sites inherently amplify them. The internet’s “amplification (and platforms’ facilitation of it) is a key reason that deepfakes have drawn public attention and one of the reasons they have the potential to erode the integrity of elections.”²⁰¹

Repealing Section 230 would not stop the spread of deepfakes, and would instead create a slew of alarming free speech implications, which are well beyond the scope of this Note. However, allowing platforms to abdicate any responsibility for the spread of deepfakes, and instead forcing litigants to track down individual entities, almost certainly guarantees very few parties will ever be held accountable for relevant harms.

VI. CONCLUSION

Technology is ever-changing—constantly racing itself to go farther, do greater things, and achieve more. How society interacts with technology is also continuously evolving, for both better and worse. The technological advancements deepfakes offer are remarkable. They have been widely used in the entertainment sphere, and present numerous opportunities for those struggling with grief and disability.²⁰² But their ability to distort the truth, and to make that

198. Chesney & Citron, *supra* note 10, at 1796.

199. *See Section 230 of the Communications Decency Act, supra* note 181.

200. Zoe Kleinman, *What Is Fake News and How Can You Identify It?*, BBC NEWS (Nov. 12, 2018), <https://www.bbc.com/news/av/technology-46149888>.

201. Nicholas Diakopoulos & Deborah G. Johnson, *Anticipating and Addressing the Ethical Implications of Deepfakes in the Context of Elections*, 23 NEW MEDIA & SOCIETY (forthcoming 2021) (manuscript at 6), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3474183.

202. Chesney & Citron, *supra* note 10, at 1771.

distortion seem factual, opens the door to a myriad of dystopian possibilities.

A.B. 730 is California's first attempt to address those possibilities. Its strengths lie in its intent and definitions, but its execution amounts to little more than a failure. The redundancies it presents could be effectively addressed by incorporating manipulated media into already-existing forms of law, such as defamation. Its constitutional flaws present a greater challenge to enforcement, but they could be overcome through revisions and narrowing. But the truly critical failing of A.B. 730 lies in its implementation. A law that cannot be enforced—even slightly—serves no purpose at all.

The time for proactive deepfakes legislation has already arrived, and it is essential that states (and ideally, the federal government) begin to address manipulated media. Our nation's best aspects—the press, the democratic process, fair elections—all rely on the public maintaining a clear understanding of what is true, not what is “fake news.” Strong legislation will be needed to achieve this, but A.B. 730 is not the template upon which to base future regulation.