EXPLORING CURRENT AND POTENTIAL SOLUTIONS

The Rise of Deepfakes in Legislative, Legal, and Technological Arenas

By Omid Asadi

The rapid rise of deepfake technology, driven by advancements in artificial intelligence (AI), presents significant challenges to intellectual property (IP) and trademark enforcement. Deepfakes, created using machine learning algorithms like Generative Adversarial Networks (GANs), generate hyper-realistic yet entirely fabricated digital content. These deepfakes have complicated the already intricate landscape of IP protection—particularly on social media platforms—where misinformation, fraud, and privacy violations are growing concerns. As these technologies evolve and become more accessible, distinguishing between genuine and manipulated media has become increasingly difficult. This paper examines the impact of deepfakes on IP and trademark enforcement, highlighting the shortcomings of current legal frameworks and enforcement mechanisms. It reviews federal and state legislative efforts and assesses the role of technology corporations in detecting and preventing deepfake content. Despite some progress, existing measures remain insufficient to address the rapidly advancing capabilities of deepfakes. To mitigate these challenges, the paper proposes a comprehensive approach that includes expanding legislative frameworks, enhancing judicial training, and investing in advanced detection technologies. It also emphasizes the importance of public awareness campaigns and the need for tech companies to enforce strict policies against deepfake misuse. By fostering collaboration among governments, legal systems, and the tech industry, a robust framework can be established to protect creators' rights, uphold digital media integrity, and maintain public trust in the face of these evolving threats.

I. Introduction

Today's rapid technological advancements have created complications and unprecedented challenges for the landscape of intellectual property and trademark enforcement. The proliferation of Artificial Intelligence (AI) and deepfake technologies on social media platforms has significantly altered the dynamics of content creation and dissemination.[1] Deepfakes can produce hyper-realistic digital content, especially by utilizing machine learning algorithms like Generative Adversarial Networks (GANs). GANs are generators that create new data resembling the training data, producing videos and audio recordings that are often indistinguishable from genuine material.[2]

1 Buffett Institute for Global Affairs, "The Rise of Artificial Intelligence and Deepfakes," Northwestern University, July, 2023, https://buffett.northwestern.edu/documents/buffett-brief_the-rise-of-ai-and-deepfake-technology.pdf.

2 "Science & Tech Spotlight: Deepfakes," U.S. Government Accountability Office, February, 2020, https://www.gao.gov/assets/gao-20-379sp.pdf.

The recent surge in the use of these technologies has led to numerous high-profile pieces of legislation of IP and copyright infringements, highlighting the urgent need for effective enforcement strategies.[3]

This research aims to navigate the intricate landscape of IP and copyright enforcement in the context of AI and deepfakes on social media. It will explore the current legal frameworks, assess the effectiveness of existing enforcement mechanisms, and propose innovative solutions to address these challenges. By focusing on legislation, case studies, and previous research on the rise of Artificial Intelligence and its influence on IP law, this study will provide a comprehensive understanding of the issue and offer practical recommendations for policymakers and content creators. While deepfakes and AI technologies present certain benefits in areas like accessibility and creative industries, their potential for misuse necessitates comprehensive solutions across the legal system, government policies, and technological advancements. As we delve into this complex issue, the goal is to illuminate a path forward, ensuring robust IP protection in the digital age and safeguarding the rights of creators in an increasingly automated world.

II. Prolific rise of deepfakes

Prior to proposing solutions to combat deepfake technologies and their impact on intellectual property and copyright enforcement, it is crucial to first understand the rise of deepfakes in social media and content creation. Deepfake technology emerged publicly in 2017, with origins rooted in advancements in artificial intelligence and machine learning. The technology gained traction when Reddit users shared videos generated by algorithms capable of superimposing faces onto existing videos with startling realism.[4] This marked the beginning of a rapid and widespread proliferation, fueled by the accessibility of deep learning tools and open-source platforms. Since then, deepfakes have expanded beyond novelty and entertainment, infiltrating areas such as political disinformation, fraud, and copyright infringement; this has made their regulation and mitigation all the more pressing.[5] In fact, the Department of Homeland Security reports that the number of deepfake videos increased by 84% from the beginning to the end of 2019.[6] Since 2019, this rapid rise has only become more profound. In 2023, deepfake fraud materials and imitations increased by 3,000%.[7] This rise can be attributed to several key developments in AI and machine learning. Over the past decade, advancements in GANs have enabled the creation of highly realistic synthetic media. Initially, this technology was used for entertainment and novelty purposes.[8] Considering the parallel rise of both Generative Adversarial Networks and deepfake fraud materials, their correlation is evident. However, as the technology became more sophisticated and accessible, its potential for misuse became apparent, and individuals began utilizing this technology for personal gain or to harm others. These fields in which individuals harm others through deepfakes include various critical areas. In elections, deepfakes are used to undermine democratic processes by spreading misinformation and manipulating voter opinions through false representations of political figures.[9] In scams and fraud, cybercriminals use deepfakes to create realistic videos or voice recordings to deceive victims into transferring money or disclosing sensitive information.[10] Additionally,

3 Lukas Whittaker et al., "The Rise of Deepfakes: A Conceptual Framework and Research Agenda for Marketing," *Australasian Marketing Journal* 29, no. 3 (2021), https://doi.org/10.1177/1839334921999479.

4 Meredith Somers, "Deepfakes, Explained," MIT Sloan, July 21, 2020, https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.

5 Ki Hong et al., "Deep Concerns Over Political Deepfakes," *Reuters*, May 20, 2024, https://www.reuters.com/legal/legalindustry/deep-concerns-over-political-deepfakes-2024-05-20/.

6 "Increasing Threat of Deepfake Identities," Department of Homeland Security, accessed July 18, 2024, https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.

7 "The Rise of Deepfakes: Navigating Their Impact on Reputation and Business," Mishcon de Reya, March 20, 2024, https://www.mishcon.com/news/the-rise-of-deepfakes-navigating-their-impact-on-reputation-and-business.

8 Joseph Rocca, "Understanding Generative Adversarial Networks (GANs)," *Towards Data Science*, March 21, 2021, https://towardsdatascience.com/understanding-generative-adversarial-networks-gans-cd6e4651a29.

9 N. David Bleisch, "Deepfakes and American Elections," American Bar Association, May 6, 2024, https://www.americanbar.org/groups/public_interest/election_law/american-democracy/our-work/deepfakes-american-elections/.

10 Melissa Dittmann Tracey, "Scammers Use Agent Deepfakes to Fool Buyers, Sellers," *Realtor Magazine Media*, National Association of Realtors, March 7, 2024, https://www.nar.realtor/magazine/real-estate-news/technology/scammers-use-agent-deepfakes-to-fool-buyers-sellers.

in the corporate world, deepfakes facilitate espionage by impersonating key personnel to extract confidential information, leading to financial losses and competitive disadvantages.[11] This major increase in the potential for misinformation and the erosion of trust in digital media are profound concerns.

A. Potential applications of deepfakes

While deepfakes are often associated with their potential for misuse, there are notable applications to this technology that should not be overlooked. For instance, deepfakes can serve as powerful tools for accessibility, enabling realistic simulations that aid individuals with disabilities. For example, deepfake technology can recreate the voices of individuals who have lost their ability to speak, offering a means of communication that is more personal and effective than traditional text-to-speech systems.[12] Moreover, the entertainment industry can harness deepfakes to create performances by deceased or non-touring artists, providing new content and experiences for audiences.[13] This technology can also be used in filmmaking to de-age actors or create realistic digital doubles, enhancing creative possibilities and storytelling. Additionally, deepfakes have educational applications, creating historical re-enactments or simulations that bring historical figures to life and provide engaging and immersive learning experiences.[14]

The US Copyright Office has recognized these potential benefits in its recent report. The report highlights how digital replicas, enabled by deepfake technology, can serve as accessibility tools for individuals with disabilities and enable performances by deceased or non-touring artists, enriching the cultural and creative landscape.[15] The ability to recreate voices and likenesses can also offer significant educational value, allowing for immersive and interactive learning experiences.

Despite these benefits, the threat posed by deepfakes remains significant, particularly in the realms of misinformation, fraud, and personal privacy violations. The same US Copyright Office report underscores the significant harms that unauthorized digital replicas can cause, including the loss of work or income for performers, potential for fraud, and defamation.[16] This dual nature of deepfakes, offering both innovative possibilities and substantial risks, necessitates a balanced approach in regulation.

III. Current approaches

Given this rise of deepfake technology and its associated risks, it is crucial to explore the current legislative measures which address these challenges. Technology companies, governments, and academic institutions have begun to recognize the severity of the issue, and are taking steps to combat the misuse of deepfake technology. Considering research institutions and technology companies in particular, there have been notable efforts to create algorithms that can detect subtle inconsistencies in deepfake videos: unnatural eye movements, lighting discrepancies, and facial asymmetries.[17] These companies, along with several other social media platforms, have

---

11 Roy Maurer, "Deepfake Scams Expose Employers to Big Risks." *SHRM*, February 20, 2024. https://www.shrm.org/topics-tools/news/technology/deepfake-scams-expose-employers-risks.

12 Dan Patterson, "Deepfakes for Good? How Synthetic Media Is Transforming Business," *TechInformed*, October 5, 2023, https://techinformed.com/deepfakes-for-good-how-synthetic-media-is-transforming-business/.

13 Beena Ammanath, "We Must Build a Case for Trustworthy AI Synthetic Content," *World Economic Forum*, May 30, 2024, https://www.weforum.org/agenda/2024/05/why-we-need-to-look-beyond-deepfakes-to-benefit-from-synthetic-content-technology/.

14 Dominic Lees, "Deepfakes Are Being Used for Good – Here's How," *Connecting Research*, University of Reading, February 7, 2023, https://research.reading.ac.uk/research-blog/deepfakes-are-being-used-for-good-heres-how/.

15 *Copyright and Artificial Intelligence, Part 1: Digital Replicas* (U.S. Copyright Office, 2024), https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf.

16 Nora Scheland, "Inside the Copyright Office's Report, 'Copyright and Artificial Intelligence, Part 1: Digital Replicas,'" *Library of Congress Blogs*, August 6, 2024, https://blogs.loc.gov/copyright/2024/08/inside-the-copyright-offices-report-copyright-and-artificial-intelligence-part-1-digital-replicas/.

17 Drew Turney, "New AI Algorithm Flags Deepfakes with 98% Accuracy — Better than Any Other Tool out There Right Now," *LiveScience*, June 24, 2024, https://www.livescience.com/technology/artificial-intelligence/new-ai-algorithm-flags-deepfakes-with-98-accuracy-better-than-any-other-tool-out-there-right-now.

explicitly prohibited the use of deepfake technology in their terms of service agreements.[18] They have made it clear that any violation of these terms will result in severe penalties, underscoring their commitment to combating the misuse of this technology.[19]

On the legislative front, both federal and state governments have begun taking steps to tackle this issue.[20] Until very recently, these pieces of legislation have largely overlooked holding creators and distributors of deepfake content accountable, prioritizing informing audiences and ensuring transparency instead. In 2019, Congress passed the Deepfake Report Act, which requires the Science and Technology Directorate in the Department of Homeland Security to report on the state of digital content forgery technology.[21] In the years following its enactment, the DHS has released several reports highlighting the increasing sophistication of deepfake technologies and their implications for both national and international security.[22] These reports have emphasized the need for enhanced detection and attribution methods, as well as the development of legal and regulatory frameworks to address the challenges posed by deepfakes.[23] The evolving policy landscape underscores the urgency of balancing technological innovation with ethical and legal safeguards to mitigate the potential harms of deepfake content.

The federal government has also overseen the passage and enforcement of the Identifying Outputs of Generative Adversarial Networks Act (IOGAN Act) in 2019, which focuses on funding research and development of technologies capable of detecting deepfakes. This act supports partnerships between government agencies, academic institutions, and private companies to advance the tools needed to identify and mitigate the impact of deepfake media.[24] As a result of the passage of the IOGAN Act, the National Science Foundation has launched various research projects, and the National Institute of Standards and Technology has developed and published technical guidelines and frameworks to manage the risks associated with generative AI and deepfakes.[25] These frameworks provide comprehensive guidance on detecting and mitigating the misuse of deepfake technologies.[26]

Another piece of legislation introduced to promote transparency and information for consumers of digital content is the Deepfakes Accountability Act of 2023. Congresswoman Yvette Clark of New York proposed legislation to criminalize the creation and distribution of deepfake content.[27] Her proposal, the Deepfakes Accountability Act, mandates that any deepfake content must be clearly labeled to inform viewers of its synthetic nature, thereby promoting transparency and accountability.[28] As of July 2024, this legislation has yet to be voted on or discussed in Congress.[29]

---

18 Kavyasri Nagumotu, "Deepfakes Are Taking Over Social Media: Can the Law Keep Up?" (JD diss., University of New Hampshire, 2022), https://law.unh.edu/sites/default/files/media/2022/06/nagumotu_pp113-157.pdf.

19 "Social Media Companies Have Seven Days to Tweak Terms of Use Around Deepfakes: Rajeev Chandrasekhar," *The Economic Times*, November 25, 2023, https://economictimes.indiatimes.com/tech/technology/social-media-companies-have-seven-days-to-tweak-terms-of-use-around-deepfakes-rajeev-chandrasekhar/articleshow/105481813.cms?from=mdr.

20 "Deceptive Audio or Visual Media ('Deepfakes') 2024 Legislation," *National Conference of State Legislatures*, accessed August 15, 2024, https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation.

21 "S. 2065 (116th): Deepfake Report Act of 2019," GovTrack, October 28, 2019, https://www.govtrack.us/congress/bills/116/s2065/text.

22 William A. Galston, "Is seeing still believing? The deepfake challenge to truth in politics," *Brookings*, January 8, 2020, https://www.brookings.edu/articles/is-seeing-still-believing-the-deepfake-challenge-to-truth-in-politics/.

23 Michelle M. Graham, "Deepfakes: Federal and State Regulation Aims to Curb a Growing Threat," Thomson Reuters, June 26, 2024, https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/.

24 "S.2904 - IOGAN Act," Library of Congress, accessed July 25, 2024, https://www.congress.gov/bill/116th-congress/senate-bill/2904.

25 "AI and IoT Legislative Developments: First Quarter 2019," Covington, May 1, 2019, https://www.cov.com/-/media/files/corporate/publications/2019/04/ai-iot-legislative-developments-first-quarter-2019.pdf.

26 "AI Risk Management Framework," National Institute of Standards and Technology, last modified April 30, 2024, https://www.nist.gov/itl/ai-risk-management-framework.

27 "US - HR3230," BillTrack50, accessed August 15, 2024, https://www.billtrack50.com/billdetail/1132741.

28 Dan Kalmowitz, "Clarke Leads Legislation to Regulate Deepfakes," Congresswoman Yvette Clarke, September 21, 2023, https://clarke.house.gov/clarke-leads-legislation-to-regulate-deepfakes/.

29 "H.R.2395 - DEEP FAKES Accountability Act," Library of Congress, accessed July 25, 2024, https://www.congress.gov/bill/117th-congress/house-bill/2395.

In July 2024, the United States Senate unanimously passed the Disrupt Explicit Forged Images and Non-Consensual Edits (DEFIANCE) Act.[30] This bipartisan legislation is a significant step in combating the rise of this technology, giving victims the ability to sue anyone who creates, shares, or receives nonconsensual sexually explicit deepfakes depicting them.[31] As Senator Dick Durbin noted, ". . . current laws don't apply to deepfakes, leaving women and girls who suffer from this image-based sexual abuse without a legal remedy."[32] Following the bill's passage, he further emphasized on X, "It's time to give victims their day in court and the tools they need to fight back."[33] Durbin's statements highlight that, despite recent legislative efforts, the laws have not kept pace with the rapid spread of this abusive content. This underscores the urgent need for effective legal remedies.

State and local governments have also proposed measures to address the deepfake threat. In California, in July 2024, State Senator Aisha Wahab introduced Senate Bill 926.[34] This bill aims to build upon existing laws by updating criminal statutes to include images made or altered through digitization.[35] Additionally, the recent California Assembly Bill 602 would establish a private cause of action against individuals who either create and intentionally disclose deepfake material without the individual's consent or disclose such material knowing that the individual did not consent to its creation or distribution.[36] If AB 602 passes in its current form, a successful plaintiff can recover economic and noneconomic damages, including emotional distress, or statutory damages ranging from $1,500 to $30,000, or up to $150,000 if the act was committed with malice.[37]

New York has also taken decisive action against the dissemination of AI-generated explicit images.[38] In October 2023, Governor Hochul signed bill S1042A into law, making it illegal to disseminate deepfake videos without the consent of the person depicted.[39] This new law imposes penalties of up to one year in jail and a $1,000 fine for those found guilty, and it also grants victims the right to pursue legal action against perpetrators.[40] Sponsoring Senator Michelle Hinchey emphasized the importance of this legislation, stating that "this is an entirely new realm of digital violation that demands vigilant attention and new legislative protections. That's why we've taken decisive action not only to outlaw this malicious practice but also to broaden the ban to anyone who circulates fake images without a person's consent. My bill sends a strong message that New York won't tolerate this form of abuse."[41] These efforts by state governments are major steps to tackling this pressing issue, and they have continued to gain relevancy and momentum especially due to continued efforts by the federal government.

---

30 Lauren Feiner, "The Senate Passed a Bill Cracking Down on Sexually Explicit Deepfakes," *The Verge*, July 24, 2024, https://www.theverge.com/2024/7/24/24205275/senate-passes-defiance-act-non-consensual-intimate-ai-deepfakes.

31 "S.3696 - DEFIANCE Act of 2024," Library of Congress, accessed July 25, 2024, https://www.congress.gov/bill/118th-congress/senate-bill/3696.

32 "Durbin Celebrates Passage Of His Bill To Tackle Nonconsensual, Sexually-Explicit Deepfakes In Speech On The Senate Floor," U.S. Senator Dick Durbin of Illinois, July 25, 2024, https://www.durbin.senate.gov/newsroom/press-releases/durbin-celebrates-passage-of-his-bill-to-tackle-nonconsensual-sexually-explicit-deepfakes-in-speech-on-the-senate-floor.

33 "The Defiance Act of 2024," U.S. Senator Dick Durbin of Illinois, accessed July 25, 2024, https://www.durbin.senate.gov/imo/media/doc/DEFIANCE%20Act%20one%20pager%20051324.pdf.

34 "California SB926," TrackBill, PolicyEngage, accessed August 15, 2024, https://trackbill.com/bill/california-senate-bill-926-crimes-distribution-of-intimate-images/2487809/.

35 Anthony David Sierra, "California Deepfake Laws First in Country to Take Effect," *Data Dive*, Akin, January 20, 2020, https://www.akingump.com/en/insights/blogs/ag-data-dive/california-deepfake-laws-first-in-country-to-take-effect.

36 "AB-602 Depiction of Individual Using Digital or Electronic Technology: Sexually Explicit Material: Cause of Action," California Legislative Information, October 4, 2019, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602.

37 Titus Wu, "California Looks to Boost Deepfake Protections before Elections," *Bloomberg Law News*, December 15, 2023, https://news.bloomberglaw.com/artificial-intelligence/california-looks-to-boost-deepfake-protections-before-elections.

38 Olivia Loftin, "Does NY Protect against the Distribution of Deepfake Pornography?," Romano Law, June 20, 2024, https://www.romanolaw.com/does-new-york-protect-against-the-distribution-of-deepfake-pornography/.

39 "Governor Hochul Continues New York's Leadership on Artificial Intelligence with Nation-Leading Actions to Protect Against Deceptive Uses of AI," Governor Kathy Hochul, February 15, 2024, https://www.governor.ny.gov/news/governor-hochul-continues-new-yorks-leadership-artificial-intelligence-nation-leading-actions.

40 Michelle Hinchey, "Hinchey Bill to Ban Non-Consensual Deepfake Images Signed into Law," The New York State Senate, October 2, 2023, https://www.nysenate.gov/newsroom/press-releases/2023/michelle-hinchey/hinchey-bill-ban-non-consensual-deepfake-images.

41 Zach Williams, "NY Governor Floats Private Right of Action for AI Deepfakes," *Bloomberg Law News*, February 15, 2024, https://news.bloomberglaw.com/artificial-intelligence/ny-gov-hochul-proposes-private-right-of-action-for-ai-deepfakes.

While significant strides have been made in combating the misuse of deepfake technology through legislative measures at both the federal and state levels, these efforts still fall short in addressing the rapid evolution and sophistication of deepfake technologies. For example, these existing laws struggle to keep pace with the rapid advancements in AI, especially with new deepfake technology targeting the voices of elected officials and influencing modern elections.[42] As deepfake technology continues to improve, the legal framework struggles to adapt quickly enough—resulting in a continuous game of catch-up. The need for continuous adaptation and enhancement of legal frameworks and enforcement mechanisms remains critical.

IV. Proposed solutions

The rapid advancement of deepfake technology has created major challenges for intellectual property and copyright enforcement. To address these issues effectively, we must adopt a comprehensive approach that encompasses the legal system, federal and state governments, and major tech companies. This section will explore a range of proposed solutions, each aimed at mitigating the negative impacts of deepfakes and ensuring protection for intellectual property rights.

A. Proposed solutions for federal and state governments

As deepfake technology evolves, so too must our legal and regulatory frameworks to effectively mitigate the associated risks. These strategies include expanding legislation, strengthening enforcement mechanisms, launching public awareness campaigns, and supporting research and development. Additionally, recent initiatives by the US Copyright Office to address issues related to digital replicas provide valuable insights and highlight the importance of a proactive approach.

Governments should continue to build on the precedent set by recent legislation, such as the DEFIANCE Act, by introducing more comprehensive laws targeting the creators and distributors of deepfake content. These laws should not be limited to addressing revenge porn or sexually explicit content but should also cover other forms of harmful deepfakes, such as those used for political manipulation, fraud, or defamation. Expanding the scope of these laws is essential to protect individuals and institutions from a wide range of malicious uses of deepfake technology. The newly introduced Digital Integrity in Democracy Act by Senator Peter Welch of Vermont focuses on enhancing the transparency and accountability of digital content.[43] This Act mandates that any digital content created using AI, including deepfakes, must be clearly labeled to inform viewers of its synthetic nature.[44] This transparency aims to reduce the spread of misinformation and help that consumers can distinguish between real and manipulated content.

With the passage of new legislation, there also is a need for effective enforcement of these mechanisms. Governments should allocate resources to law enforcement agencies to ensure they have the necessary tools and training to identify and prosecute deepfake related crimes. This includes investing in technology capable of detecting deepfakes and establishing specialized units within law enforcement agencies to handle these cases. By enhancing the capacity of law enforcement, governments can ensure that deepfake perpetrators are held accountable. For example, law enforcement agencies can use advanced algorithms and machine learning techniques to identify deepfake content, while specialized units can focus on investigating and prosecuting these crimes.

---

42 Kevin Schaul et al., "See How AI Detection Works, and Fails, to Catch Election Deepfakes," *The Washington Post*, August 15, 2024, https://www.washingtonpost.com/technology/interactive/2024/ai-detection-tools-accuracy-deepfakes-election-2024/.

43 Tim, "Welch Introduces 'Digital Integrity' Bill to Counter False Election Administration Content," *Vermont Business Magazine*, August 5, 2024, https://vermontbiz.com/news/2024/august/05/welch-introduces-digital-integrity-bill-counter-false-election-administration.

44 Lauren Denham, "Welch Leads Colleagues in Introducing Bill to Increase Accountability from Social Media Platforms That Knowingly Host False Election Administration Content," Jeff Merkley Senator for Oregon, August 5, 2024, https://www.merkley.senate.gov/welch-leads-colleagues-in-introducing-bill-to-increase-accountability-from-social-media-platforms-that-knowingly-host-false-election-administration-content/.

Governments have a crucial role to play in raising public awareness about the dangers of deepfake technology by launching large-scale, well-coordinated education campaigns. These campaigns would serve to inform citizens about the risks posed by deepfakes, such as their potential use in disinformation, identity theft, political manipulation, and other forms of cybercrime. By educating the public, governments can empower individuals to better identify and respond to deepfake content, ultimately reducing the negative impact of this technology on society. Public awareness campaigns should leverage multiple platforms to reach a diverse audience, including television, social media, radio, and print media. They could feature real-world examples of how deepfakes have been used maliciously to illustrate the severity of the problem. Additionally, these campaigns could break down the technical signs of deepfake content—irregular blinking, mismatched audio-visual cues, unnatural facial expressions, and lighting inconsistencies—helping everyday users understand what to look for when assessing the authenticity of a video or image. Interactive workshops and seminars could also play a significant role in educating specific groups such as students, senior citizens, and professionals in high-risk fields (journalism, law enforcement, and politics). By tailoring workshops to different demographics, governments can provide practical, hands-on training in recognizing and reporting deepfake content. The Media Literacy in the Age of Deepfakes project by MIT is an example of a demonstrated effectiveness in improving participants' ability to detect manipulated media. Through interactive workshops and digital tools, the program equips individuals with practical skills to identify deepfake content, enhancing critical thinking and skepticism toward suspicious media. Empirical studies linked to the project show that such training reduces the spread of disinformation and fosters digital resilience across diverse demographics.[45] This highlights the importance of integrating media literacy into public campaigns to mitigate the risks of deepfakes.

In addition to promoting public awareness campaigns, federal and state governments should also fund research initiatives aimed at developing advanced technologies to detect and prevent the misuse of deepfakes. Collaborations between government agencies, academic institutions, and private companies can drive innovation in this field and provide effective solutions to combat deepfake technology. For example, research grants and funding programs can support projects that explore new detection methods, improve existing technologies, and develop tools for verifying the authenticity of digital content. One notable research grant that exemplifies the type of initiative governments should support is the Defense Advanced Research Projects Agency's (DARPA) Media Forensics (MediFor) program.[46] The program brings together researchers from academic institutions, government agencies, and private companies to create automated tools that can assess the integrity of visual media. Funded through research contracts, the program requires participants to meet specific deliverables, including progress reports and technology demonstrations.[47] Additionally, the grant terms include data-sharing requirements and outline the handling of intellectual property, ensuring that innovations can be effectively transitioned to operational use.[48] By supporting initiatives like the MediFor program, the government not only fosters innovation in media forensics but also strengthens its ability to address the growing threats posed by deepfake technology, ensuring a more secure and trustworthy digital landscape.

B. Proposed solutions for the legal system

The legal system plays a crucial role in addressing the challenges posed by deepfake technology. Since deepfakes are a relatively new phenomenon, courts often have to rely on current legislation and the enactment of new laws to determine the criminality of such acts. One proposed solution for the legal system is to reinterpret existing laws to cover deepfake related offenses more comprehensively. This would include interpreting and applying current statutes on copyright, defamation, and individual privacy protections to explicitly include the creation

45 "Media Literacy in the Age of Deepfakes," Center for Advanced Virtuality, MIT, accessed October 18, 2021, https://deepfakes.virtuality.mit.edu/.

46 "MediFor: Media Forensics," DAPRA, accessed August 15, 2024. https://www.darpa.mil/program/media-forensics.

47 Taylor Hatmaker, "DARPA Is Funding New Tech That Can Identify Manipulated Videos and 'Deepfakes,'" *TechCrunch*, April 30, 2018, https://techcrunch.com/2018/04/30/deepfakes-fake-videos-darpa-sri-international-media-forensics/.

48 Tajha Chappellet-Lanier, "DARPA Wants to Tackle 'Deepfakes' with Semantic Forensics," *FedScoop*, August 7, 2019, https://fedscoop.com/darpa-semantic-forensics-proposers-day/.

and distribution of deepfakes as punishable offenses. Amending copyright laws to include unauthorized digital replicas can provide clearer guidelines for prosecution and enforcement, ensuring that creators and distributors of deepfakes are held accountable. For instance, existing copyright laws protect original works of authorship, but they do not explicitly address the complexities introduced by deepfake technology.[49] State-level laws, such as Assembly Bill 602 in California, target specific uses of deepfakes, like those intended to influence elections or violate an individual's privacy.[50] However, this law and similar proposals vary widely in scope and effectiveness, with some focusing only on certain types of deepfakes, such as political or non-consensual explicit content, leaving other harmful uses inadequately addressed.[51] By updating these laws to consider unauthorized digital replicas as infringements, courts can more effectively adjudicate cases involving deepfakes.

In addition to reinterpreting existing laws, enhancing judicial training is essential. By integrating deepfake-related topics into law school curricula and providing ongoing education for judges and legal practitioners, the legal community can develop a deeper understanding of the technical aspects of deepfake technology. Judges should be equipped with specific knowledge in several key areas to effectively adjudicate cases involving deepfakes. First, they need a robust understanding of the technical aspects of how deepfakes are created, including the use of AI and machine learning algorithms, as well as the potential markers of deepfake content that distinguish it from authentic media. This understanding is crucial for evaluating expert testimony and the reliability of evidence presented in court. Furthermore, judges should be aware of the various types of harm deepfakes can cause, ranging from reputational damage and privacy violations to their potential use in fraud, extortion, and electoral manipulation. By recognizing the wide-ranging impacts, judges can better assess the severity of the cases before them.

The legal system must thoroughly examine current legal frameworks to identify areas where deepfakes may already fall under existing statutes, such as those related to fraud, defamation, and privacy violations. The current legal framework includes several pieces of legislation aimed at addressing the misuse of deepfakes. For instance, the DEEPFAKES Accountability Act and the Deepfake Report Act of 2019 both aim to promote transparency and accountability, thereby reducing the spread of misinformation. These reports have highlighted the increasing sophistication of deepfakes and the associated risks, thereby informing the public and policymakers about the urgent need for robust legal frameworks. Despite these efforts, the effectiveness of current laws is often limited by their scope and the rapid evolution of deepfake technology.

C. Proposed solutions for big tech companies

As the prevalence and sophistication of deepfake technology increase, tech companies must take proactive measures to combat its misuse. These strategies include implementing advanced detection technologies, enforcing strict policies, ensuring transparency, collaborating with governments and academia, and providing user education and tools. Additionally, recent initiatives by tech giants highlight the importance of industry leaders taking a proactive stance in shaping AI regulation and technology development.[52] These measures are not only vital for safeguarding users but also essential for maintaining the integrity and reputation of the companies themselves. By addressing the deepfake challenge head-on, tech companies can enhance user trust, comply with emerging regulations, and position themselves as leaders in responsible AI development.

Initially, tech companies should invest in and deploy sophisticated algorithms and machine learning models capable of detecting deepfake content. These technologies can analyze videos and audio for inconsistencies, such

49 Liz Hockley, "US Copyright Office Urges New Law to Tackle 'Serious Threat' from Deepfakes," *World Intellectual Property Review*, August 2, 2024, https://www.worldipreview.com/copyright/us-copyright-office-urges-new-law-to-tackle-serious-threat-from-deepfakes.

50 Samuel Dordulian, "Can I Sue as a Victim of Deepfake Porn?," Dordulian Law Group, January 4, 2024, https://www.dlawgroup.com/legal-options-for-california-deepfake-porn-victims-explained/.

51 K.C. Halm et al., "Two New California Laws Tackle Deepfake Videos in Politics and Porn," *Media Law Monitor*, Davis Wright Tremaine, February 28, 2020, https://www.dwt.com/blogs/media-law-monitor/2020/02/two-new-california-laws-tackle-deepfake-videos-in.

52 Kalley Huang, "Here's How Big Tech Is Tackling Deepfakes," *The Information*, March 7, 2024, https://www.theinformation.com/articles/heres-how-big-tech-is-tackling-deepfakes.

as unnatural eye movements or facial asymmetries, that indicate manipulation. By continuously improving these detection methods, tech companies can stay ahead of increasingly realistic deepfakes. For instance, companies can leverage AI to identify subtle signs of tampering that are not easily detectable by the human eye, thereby enhancing the overall accuracy and reliability of their detection systems. One promising advancement in this area is the development of SynthID, a tool launched in partnership with Google Cloud. SynthID is designed to watermark and identify AI-generated images. This technology embeds a digital watermark directly into the pixels of an image, making it imperceptible to the human eye but detectable for identification. This innovative approach allows tech companies to track and verify AI-generated content, ensuring greater accountability and traceability. Currently, SynthID is being released to a limited number of Vertex AI customers using Imagen, one of the latest text-to-image models that creates photorealistic images from input text.[53] As this technology continues to develop, it could become a vital tool for tech companies and consumers to recognize deepfake content.

In addition to providing software for combatting this technology, social media platforms and other tech companies should establish and enforce strict policies against the creation and distribution of deepfake content. This includes clear terms of service that prohibit the use of deepfake technology for harmful purposes and severe penalties for violations, such as account suspension or banning. By setting clear guidelines and enforcing them consistently, tech companies can deter malicious actors from using their platforms to spread deepfake content. Moreover, these policies should be regularly reviewed and updated to address new and emerging threats posed by advancements in deepfake technology. Tech companies must also demonstrate transparency in their efforts to combat deepfakes. They should regularly publish reports detailing the measures they have taken, the number of deepfake incidents detected and removed, and the effectiveness of their detection technologies. This transparency can help build public trust and show a genuine commitment to addressing the issue. Quarterly or annual transparency reports can provide insights into the volume and types of deepfake content encountered, as well as the success rates of different detection and mitigation strategies. Additionally, as long as these tech companies are able to demonstrate strict enforcement of these policies, they should not be held liable for harm caused by deepfake activity on their platforms. This will incentivize these companies to advance these policies and strengthen their enforcement to target deepfakes.

Big tech companies should also collaborate with government agencies and academia institutions to stay ahead of deepfake technology. These partnerships can facilitate the sharing of knowledge, resources, and technological advancements, enabling a more coordinated and effective response to the threat posed by deepfakes. For example, joint research initiatives can focus on developing new detection techniques, improving existing technologies, and exploring the ethical implications of deepfakes. Additionally, collaborative efforts can help standardize best practices and create a unified front against the misuse of deepfake technology. Microsoft has already taken a proactive role in addressing the challenges posed by AI and deepfake technology.[54] In a recent document, Microsoft discussed proposals for Congress to pass laws that make it illegal to use AI-generated voices and images to defraud people and require AI companies to build technology to identify fake AI images made with their products.[55] Specifically, Microsoft proposes a "deepfake fraud statute" that will give law enforcement officials a legal framework to prosecute AI-generated scams and fraud. Additionally, they are calling on lawmakers to "ensure that our federal and state laws on child sexual exploitation and abuse and non-consensual intimate imagery are updated to include AI-generated content."[56] Microsoft's recommendations, although not depicting a partnership with tech companies and the government, presents a major step forward for proposing companies and the federal government working with each other to combat the misuse of this technology.[57]

---

53 Sven Gowal and Pushmeet Kohli, "Identifying AI-Generated Images with SynthID," *Google DeepMind*, August 29, 2023, https://deepmind.google/discover/blog/identifying-ai-generated-images-with-synthid/.

54 Tom Warren, "Microsoft Wants Congress to Outlaw AI-Generated Deepfake Fraud," *The Verge*, July 30, 2024, https://www.theverge.com/2024/7/30/24209404/microsoft-deepfake-congress-lawmakers-ai-fraud.

55 Tom Burt and Eric Horvitz, "New Steps to Combat Disinformation," *Microsoft on the Issues*, Microsoft, September 1, 2020, https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/.

56 Warren, "Microsoft Wants Congress."

57 Gowal and Kohli, "Identifying AI-Generated Images."

Tech companies should prioritize equipping users with accessible tools and resources to detect and report deepfake content, fostering a collaborative effort to tackle this growing issue. By integrating educational materials—such as interactive guides, tutorials, and visual aids—into their platforms, these companies can demystify the technology behind deepfakes for everyday users. For example, tech platforms could implement user-friendly training modules that break down the common telltale signs of deepfake manipulation, such as inconsistencies in facial expressions, lip-syncing mismatches, irregular blinking, and lighting disparities that don't align with natural conditions. In addition to focusing on facial anomalies, these modules could highlight audio-visual synchronization issues—small glitches or distortions that are often present in deepfakes. Beyond simple identification, these resources should encourage proactive user involvement by making the reporting process straightforward. Tech companies could offer features that allow users to flag potential deepfakes easily, linking these reports to internal review teams or automated systems designed to scrutinize content for authenticity. By incorporating this two-tier system—education followed by action—users become an integral part of the defense against malicious deepfake use. Moreover, fostering a community-based reporting culture could increase the overall vigilance against deepfake content. Crowdsourced efforts, combined with the companies' own artificial intelligence detection systems, can enhance the speed and accuracy of identifying manipulated media. This cooperative model not only raises awareness but also builds a more resilient, informed online ecosystem that is better equipped to mitigate the harmful effects of deepfake technology, such as misinformation, harassment, and reputational damage.

V. Conclusion

The rapid evolution of artificial intelligence and deepfake technology has brought about unprecedented challenges in the realm of intellectual property and trademark enforcement, particularly on social media platforms. Deepfakes, leveraging advanced machine learning algorithms such as Generative Adversarial Networks (GANs), can create highly realistic yet fraudulent digital content, complicating the task of distinguishing between authentic and manipulated media.

Addressing these challenges requires a multifaceted approach involving the legal system, federal and state governments, and major tech companies. The legal system must adapt by reinterpreting existing laws and enhancing judicial training to comprehensively cover deepfake-related offenses comprehensively. Federal and state governments need to expand legislation, strengthen enforcement mechanisms, launch public awareness campaigns, and support research and development to stay ahead of technological advancements. Tech companies should invest in advanced detection technologies, enforce strict policies, ensure transparency, collaborate with governments and academia, and provide user education and tools.

Ultimately, the fight against deepfakes is not solely about protecting intellectual property rights; it's about preserving the foundation of trust in our digital ecosystems. As deepfake technology becomes more sophisticated, the risks extend far beyond issues of ownership—touching on the credibility of information, the authenticity of media, and the safety of individuals. By undermining the integrity of digital media, deepfakes have the potential to erode public trust in journalism, political discourse, and even personal interactions. As we move forward, sustained vigilance will be key. Deepfake technology is constantly evolving, and our societal, legal, and technological responses must adapt in tandem. By fostering a proactive and collaborative approach, we can safeguard the integrity of digital media, uphold public trust, and ensure that creators' rights are protected in an increasingly automated and complex digital world.

VI. Bibliography

Ammanath, Beena. "We Must Build a Case for Trustworthy AI Synthetic Content." *World Economic Forum*, May 30, 2024. https://www.weforum.org/agenda/2024/05/why-we-need-to-look-beyond-deepfakes-to-benefit-from-synthetic-content-technology/.

BillTrack50. "US - HR3230." Accessed August 15, 2024. https://www.billtrack50.com/billdetail/1132741.

Bleisch, N. David. "Deepfakes and American Elections." American Bar Association, May 6, 2024. https://www.americanbar.org/groups/public_interest/election_law/american-democracy/our-work/deepfakes-american-elections/.

Buffett Institute for Global Affairs. "The Rise of Artificial Intelligence and Deepfakes." Northwestern University, July, 2023. https://buffett.northwestern.edu/documents/buffett-brief_the-rise-of-ai-and-deepfake-technology.pdf.

Burt, Tom, and Eric Horvitz. "New Steps to Combat Disinformation." *Microsoft on the Issues*. Microsoft, September 1, 2020. https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/.

California Legislative Information. "AB-602 Depiction of Individual Using Digital or Electronic Technology: Sexually Explicit Material: Cause of Action." October 4, 2019. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602.

Center for Advanced Virtuality. "Media Literacy in the Age of Deepfakes." MIT, Accessed October 18, 2021. https://deepfakes.virtuality.mit.edu/.

Chappellet-Lanier, Tajha. "DARPA Wants to Tackle 'Deepfakes' with Semantic Forensics." *FedScoop*, August 7, 2019. https://fedscoop.com/darpa-semantic-forensics-proposers-day/.

Covington. "AI and IoT Legislative Developments: First Quarter 2019." May 1, 2019. https://www.cov.com/-/media/files/corporate/publications/2019/04/ai-iot-legislative-developments-first-quarter-2019.pdf.

DARPA. "MediFor: Media Forensics." Accessed August 15, 2024. https://www.darpa.mil/program/media-forensics.

Denham, Lauren. "Welch Leads Colleagues in Introducing Bill to Increase Accountability from Social Media Platforms That Knowingly Host False Election Administration Content." Jeff Merkley Senator for Oregon, August 5, 2024. https://www.merkley.senate.gov/welch-leads-colleagues-in-introducing-bill-to-increase-accountability-from-social-media-platforms-that-knowingly-host-false-election-administration-content/.

Department of Homeland Security. "Increasing Threat of Deepfake Identities." Accessed July 18, 2024. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.

Dordulian, Samuel. "Can I Sue as a Victim of Deepfake Porn?" Dordulian Law Group, January 4, 2024. https://www.dlawgroup.com/legal-options-for-california-deepfake-porn-victims-explained/.

Feiner, Lauren. "The Senate Passed a Bill Cracking Down on Sexually Explicit Deepfakes." *The Verge*, July 24, 2024. https://www.theverge.com/2024/7/24/24205275/senate-passes-defiance-act-non-consensual-intimate-ai-deepfakes.

Galston, William A. "Is seeing still believing? The deepfake challenge to truth in politics." *Brookings*, January 8, 2020. https://www.brookings.edu/articles/is-seeing-still-believing-the-deepfake-challenge-to-truth-in-politics/.

Governor Kathy Hochul. "Governor Hochul Continues New York's Leadership on Artificial Intelligence with

Nation-Leading Actions to Protect Against Deceptive Uses of AI." February 15, 2024. https://www.governor.ny.gov/news/governor-hochul-continues-new-yorks-leadership-artificial-intelligence-nation-leading-actions.

GovTrack. "S. 2065 (116th): Deepfake Report Act of 2019." October 28, 2019. https://www.govtrack.us/congress/bills/116/s2065/text.

Gowal, Sven and Pushmeet Kohli. "Identifying AI-Generated Images with SynthID." *Google DeepMind*, August 29, 2023. https://deepmind.google/discover/blog/identifying-ai-generated-images-with-synthid/.

Graham, Michelle M. "Deepfakes: Federal and State Regulation Aims to Curb a Growing Threat." Thomson Reuters, June 26, 2024. https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/.

Halm, K.C., Ambika Kumar, Jonathan Segal, and Caesar Kalinowski IV. "Two New California Laws Tackle Deepfake Videos in Politics and Porn." *Media Law Monitor*, Davis Wright Tremaine, February 28, 2020. https://www.dwt.com/blogs/media-law-monitor/2020/02/two-new-california-laws-tackle-deepfake-videos-in.

Hatmaker, Taylor. "DARPA Is Funding New Tech That Can Identify Manipulated Videos and 'Deepfakes.'" *TechCrunch*, April 30, 2018. https://techcrunch.com/2018/04/30/deepfakes-fake-videos-darpa-sri-international-media-forensics/.

Hinchey, Michelle. "Hinchey Bill to Ban Non-Consensual Deepfake Images Signed into Law." The New York State Senate, October 2, 2023. https://www.nysenate.gov/newsroom/press-releases/2023/michelle-hinchey/hinchey-bill-ban-non-consensual-deepfake-images.

Hockley, Liz. "US Copyright Office Urges New Law to Tackle 'Serious Threat' from Deepfakes." *World Intellectual Property Review*, August 2, 2024. https://www.worldipreview.com/copyright/us-copyright-office-urges-new-law-to-tackle-serious-threat-from-deepfakes.

Hong, Ki, Tyler Rosen, and Aanchal Chugh. "Deep Concerns Over Political Deepfakes." *Reuters*, May 20, 2024. https://www.reuters.com/legal/legalindustry/deep-concerns-over-political-deepfakes-2024-05-20/.

Huang, Kalley. "Here's How Big Tech Is Tackling Deepfakes." *The Information*, March 7, 2024. https://www.theinformation.com/articles/heres-how-big-tech-is-tackling-deepfakes.

Kalmowitz, Dan. "Clarke Leads Legislation to Regulate Deepfakes." Congresswoman Yvette Clarke, September 21, 2023. https://clarke.house.gov/clarke-leads-legislation-to-regulate-deepfakes/.

Lees, Dominic. "Deepfakes Are Being Used for Good – Here's How." *Connecting Research*. University of Reading, February 7, 2023. https://research.reading.ac.uk/research-blog/deepfakes-are-being-used-for-good-heres-how/.

Library of Congress. "H.R.2395 - DEEP FAKES Accountability Act." Accessed July 25, 2024. https://www.congress.gov/bill/117th-congress/house-bill/2395.

Library of Congress. "S.2904 - IOGAN Act." Accessed July 25, 2024. https://www.congress.gov/bill/116th-congress/senate-bill/2904.

Library of Congress. "S.3696 - DEFIANCE Act of 2024." Accessed July 25, 2024. https://www.congress.gov/bill/118th-congress/senate-bill/3696.

Loftin, Olivia. "Does NY Protect against the Distribution of Deepfake Pornography?" Romano Law, June 20, 2024. https://www.romanolaw.com/does-new-york-protect-against-the-distribution-of-deepfake-pornography/.

Maurer, Roy. "Deepfake Scams Expose Employers to Big Risks." *SHRM*, February 20, 2024. https://www.shrm.org/topics-tools/news/technology/deepfake-scams-expose-employers-risks.

Mishcon de Reya. "The Rise of Deepfakes: Navigating Their Impact on Reputation and Business." March 20, 2024. https://www.mishcon.com/news/the-rise-of-deepfakes-navigating-their-impact-on-reputation-and-business.

Nagumotu, Kavyasri. "Deepfakes Are Taking Over Social Media: Can the Law Keep Up?" JD diss., University of New Hampshire, 2022. https://law.unh.edu/sites/default/files/media/2022/06/nagumotu_pp113-157.pdf.

National Conference of State Legislatures. "Deceptive Audio or Visual Media ('Deepfakes') 2024 Legislation." Accessed August 15, 2024. https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation.

National Institute of Standards and Technology. "AI Risk Management Framework." Last modified April 30, 2024. https://www.nist.gov/itl/ai-risk-management-framework.

Negi, Shweta, and Shikha Upadhyay. "What the Heck Is a Deepfake?" *UVA Information Security*, Accessed July 11, 2024. https://security.virginia.edu/deepfakes.

Patterson, Dan. "Deepfakes for Good? How Synthetic Media Is Transforming Business." *TechInformed*, October 5, 2023. https://techinformed.com/deepfakes-for-good-how-synthetic-media-is-transforming-business/.

Rocca, Joseph. "Understanding Generative Adversarial Networks (GANs)." *Towards Data Science*, March 21, 2021. https://towardsdatascience.com/understanding-generative-adversarial-networks-gans-cd6e4651a29.

Schaul, Kevin, Pranshu Verma, and Cat Zakrzewski. "See How AI Detection Works, and Fails, to Catch Election Deepfakes." *The Washington Post*, August 15, 2024. https://www.washingtonpost.com/technology/interactive/2024/ai-detection-tools-accuracy-deepfakes-election-2024/.

Scheland, Nora. "Inside the Copyright Office's Report, 'Copyright and Artificial Intelligence, Part 1: Digital Replicas.'" *Library of Congress Blogs*, August 6, 2024. https://blogs.loc.gov/copyright/2024/08/inside-the-copyright-offices-report-copyright-and-artificial-intelligence-part-1-digital-replicas/.

Sierra, Anthony David. "California Deepfake Laws First in Country to Take Effect." *Data Dive*. Akin, January 20, 2020. https://www.akingump.com/en/insights/blogs/ag-data-dive/california-deepfake-laws-first-in-country-to-take-effect.

Somers, Meredith. "Deepfakes, Explained." MIT Sloan, July 21, 2020. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.

Tim. "Welch Introduces 'Digital Integrity' Bill to Counter False Election Administration Content." *Vermont Business Magazine*, August 5, 2024. https://vermontbiz.com/news/2024/august/05/welch-introduces-digital-integrity-bill-counter-false-election-administration.

Tracey, Melissa Dittmann. "Scammers Use Agent Deepfakes to Fool Buyers, Sellers." *Realtor Magazine Media*. National Association of Realtors, March 7, 2024. https://www.nar.realtor/magazine/real-estate-news/technology/scammers-use-agent-deepfakes-to-fool-buyers-sellers.

TrackBill. "California SB926." PolicyEngage, accessed August 15, 2024. https://trackbill.com/bill/california-senate-bill-926-crimes-distribution-of-intimate-images/2487809/.

The Economic Times. "Social Media Companies Have Seven Days to Tweak Terms of Use Around Deepfakes: Rajeev Chandrasekhar." November 25, 2023. https://economictimes.indiatimes.com/tech/technology/social-media-companies-have-seven-days-to-tweak-terms-of-use-around-deepfakes-rajeev-chandrasekhar/articleshow/105481813.cms?from=mdr.

Turney, Drew. "New AI Algorithm Flags Deepfakes with 98% Accuracy — Better than Any Other Tool out There Right Now." *LiveScience*, June 24, 2024. https://www.livescience.com/technology/artificial-intelligence/new-ai-algorithm-flags-deepfakes-with-98-accuracy-better-than-any-other-tool-out-there-right-now.

United Nations Academic Impact. "Promoting Intellectual Property Law to Protect Creativity." Accessed July 11, 2024. https://www.un.org/en/academic-impact/promoting-intellectual-property-law-protect-creativity.

U.S. Copyright Office. "Artificial Intelligence Study." Accessed August 1, 2024. https://www.copyright.gov/policy/artificial-intelligence/.

U.S. Copyright Office. *Copyright and Artificial Intelligence, Part 1: Digital Replicas*. July, 2024. https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf.

U.S. Copyright Office. "The Digital Millennium Copyright Act of 1998." Accessed July 11, 2024. https://www.copyright.gov/legislation/dmca.pdf.

U.S. Government Accountability Office. "Science & Tech Spotlight: Deepfakes." February, 2020. https://www.gao.gov/assets/gao-20-379sp.pdf.

U.S. Senator Dick Durbin of Illinois. "Durbin Celebrates Passage Of His Bill To Tackle Nonconsensual, Sexually-Explicit Deepfakes In Speech On The Senate Floor." July 25, 2024. https://www.durbin.senate.gov/newsroom/press-releases/durbin-celebrates-passage-of-his-bill-to-tackle-nonconsensual-sexually-explicit-deepfakes-in-speech-on-the-senate-floor.

U.S. Senator Dick Durbin of Illinois. "The Defiance Act of 2024." Accessed July 25, 2024. https://www.durbin.senate.gov/imo/media/doc/DEFIANCE%20Act%20one%20pager%20051324.pdf.

Warren, Tom. "Microsoft Wants Congress to Outlaw AI-Generated Deepfake Fraud." *The Verge*, July 30, 2024. https://www.theverge.com/2024/7/30/24209404/microsoft-deepfake-congress-lawmakers-ai-fraud.

Whittaker, Lukas, Kate Letheren, and Rory Mulcahy. "The Rise of Deepfakes: A Conceptual Framework and

Research Agenda for Marketing." *Australasian Marketing Journal* 29, no. 3 (2021): 204–14. https://doi.org/10.1177/1839334921999479.

Williams, Zach. "NY Governor Floats Private Right of Action for AI Deepfakes." *Bloomberg Law News*, February 15, 2024. https://news.bloomberglaw.com/artificial-intelligence/ny-gov-hochul-proposes-private-right-of-action-for-ai-deepfakes.

Wu, Titus. "California Looks to Boost Deepfake Protections before Elections." *Bloomberg Law News*, December 15, 2023. https://news.bloomberglaw.com/artificial-intelligence/california-looks-to-boost-deepfake-protections-before-elections.