

Ingham County Bar Association

BRIEFS



BRIEFS 25-26 #3

Upcoming Events, Page 2 | President's Message, Page 4



Prosecutors' Office

Ingham County Prosecuting Attorney, John Dewane

Michigan's Protection from Intimate Deep Fakes Act and Federal TAKE IT DOWN Act

By Lindsey M. Mead and Alexander S. Rusek



Lindsey M. Mead
lmead@fosterswift.com



Alexander S. Rusek
arusek@fosterswift.com

Fast Facts:

- Michigan's Protection from Intimate Deep Fakes Act creates a civil cause of action against creators and disseminators of sexually explicit Deep Fake images and video.
- Michigan's Protection from Intimate Deep Fakes Act creates misdemeanor and felony criminal offenses for the creation and dissemination of sexually explicit Deep Fake images and video.
- Michigan's Protection from Intimate Deep Fakes Act follows the enactment of the federal TAKE IT DOWN Act in May 2025.

Exploding onto the scene in November of 2022, generative artificial intelligence programs ("AI") (such as ChatGPT, Gemini, Grok, Midjourney, Claude, Microsoft Copilot, and many others) have gained widespread adoption in personal and professional settings alike. Concerningly, the proliferation of these sophisticated AI tools has created a new and insidious form of personal violation: the nonconsensual creation and dissemination of sexually explicit "Deep Fakes."¹

In response to the rising proliferation of Deep Fakes, the State of Michigan has moved in a bipartisan manner to address the issue by enacting Public Act

11 of 2025, titled the Protection from Intimate Deep Fakes Act (the "Act").^{2, 3} This landmark AI legislation establishes a framework of civil remedies and criminal penalties designed to hold perpetrators accountable and provide recourse for victims.

What is a "Deep Fake?"

There is no singular definition of what constitutes a Deep Fake, but commentators have described them as:

- "a video, photo, or audio recording that seems real but has been manipulated with AI. The underlying technology can replace faces, manipulate facial expressions, synthesize faces, and synthesize speech. Deepfakes can depict someone appearing to say or do something that they in fact never said or did."⁴
- "an artificial image or video (a series of images) generated by a special kind of *machine learning* called ['deep'] learning (hence the name)."⁵
- "videos, picture or audio clips made with artificial intelligence to look real. They can be used for fun, or even for scientific research, but sometimes they're used to impersonate people like politicians or world leaders, in order to deliberately mislead people."⁶

- “[a ‘deepfake’] refers to recreated media of a person’s appearance and/or voice by a type of artificial intelligence called deep learning (hence the name, deepfake).”⁷

The Protection from Intimate Deep Fakes Act aims to address the issue of AI Deep Fakes in Michigan.⁸ Under the statute, a Deep Fake is defined as “a video recording, motion-picture film, sound recording, electronic image, or photograph, or a technological representation of speech or conduct substantially derivative of such a recording, film, image, or photograph, that is not an original recording of an actual occurrence or an original photograph without substantial modification to which both of the following apply: (i) [i]t is so realistic that a reasonable person would believe it depicts speech or conduct of a depicted individual. (ii) [t]he production of it was substantially dependent on technical means, rather than the ability of another individual to physically or verbally impersonate the depicted individual.”⁹

Creation of a Civil Cause of Action

The Protection from Intimate Deep Fakes Act establishes a civil cause of action for “the nonconsensual creation or dissemination of a deep fake”.¹⁰ To bring this new cause of action, a plaintiff has the burden to prove that: (1) The “person who created or disseminated the deep fake knew or reasonably should have known that the creation, distribution, or reproduction of the deep fake would cause physical, emotional, reputational, or economic harm to an individual falsely depicted; or created or disseminated the deep fake in order to harass, extort, threaten, or cause physical, emotional, reputational,

or economic harm to an individual falsely depicted[;]” (2) The Deep Fake must realistically depict one or more of the following: “[t]he intimate parts of the depicted individual” or “[t]he depicted individual engaging in a sexual act”; and (3) The depicted individual is identifiable either “[f]rom the deep fake itself, by the depicted individual or by a reasonable individual viewing or listening to the deep fake” or “[f]rom the personal information displayed in connection with the deep fake.”¹¹

An action based on the creation or dissemination of Deep Fakes accrues at the time the depicted individual “discovers that the deep fake has been created or disseminated.”¹² The action may be filed in the county where the defendant *or* plaintiff reside *or* “where the deep fake was produced, reproduced, or stored.”¹³ Courts must allow confidential filings in this type of action, and may elect to “grant injunctive relief to maintain the confidentiality of the plaintiff using a pseudonym.”¹⁴

For cases filed asserting a civil cause of action under MCL 752.383, it is not a defense to a claim that the individual depicted in the Deep Fake consented to the creation or possession of the Deep Fake or to the voluntary transmission of the Deep Fake, whether disseminated publicly or privately, unless *both* of the following apply: (1) “[t]he consent is contained in an agreement written in plain language signed knowingly and



voluntarily by the depicted individual;” and (2) “[t]he consent includes a general description of the intimate digital depiction and, if applicable, the audiovisual work into which it will be incorporated.”¹⁵

Conversely, the Act creates multiple defenses to a civil cause of action brought for the creation or dissemination of Deep Fakes. The defenses are:

- “The creation or dissemination was made for the purpose of a criminal investigation or prosecution that is otherwise lawful.”¹⁶
- “The creation or dissemination was for the purpose of, or in connection with, the reporting of unlawful conduct.”¹⁷
- “The creation or dissemination was made in the course of seeking or receiving medical or mental health treatment, and the image is protected from further dissemination.”¹⁸

- “The deep fake related to a matter of public interest, the creation or dissemination served a lawful public purpose, the person creating or disseminating the deep fake as a matter of public interest clearly identified that the video recording, motion-picture film, sound recording, electronic image, photograph, or other item was a deep fake, and the person acted in good faith to prevent further dissemination of the deep fake.”¹⁹
- “The creation or dissemination was made for legal proceedings and was consistent with common practice in civil proceedings necessary for the proper functioning of the civil justice system, or protected by court order that prohibited any further dissemination.”²⁰

There are also other carveouts in the Act for: (1) “an interactive computer service as defined in 47 USC 230(f) (2);”²¹ (2) “[a] provider of public mobile services or private radio services;”²² (3) “[a] telecommunications network or broadband provider;”²³ and (4) “[a] provider or developer of a technology used in the creation of a deep fake, if the technology is not designed for, marketed for, or deployed for the nonconsensual creation or dissemination of deep fakes that realistically depict the intimate parts of depicted individuals or depicted individuals engaging in sexual acts, and if the provider or developer has prohibited explicit deep fake content in accordance with the provider’s or developer’s terms of service.”²⁴

Damages available for a prevailing civil action plaintiff include: (1) economic and non-economic damages, including, without limitation, financial losses

that incurred due to the creation or dissemination of the Deep Fake, as well as damages for “mental anguish, embarrassment, and humiliation[;]”²⁵ (2) an financial amount equal to any profit made by the individual found liable from the creation or dissemination of the Deep Fake;²⁶ and (3) actual court costs and fees, including reasonable attorneys’ fees.²⁷



Creation of Criminal Penalties

Aside from the civil cause of action created by the Act, the Act also creates a misdemeanor offense punishable by imprisonment for not more than one year, a fine of not more than \$3,000.00, or both, for people convicted under the Act.²⁸

To secure a conviction under the Act, there are numerous elements that a prosecutor must prove. First, it must be shown that the accused “knew or reasonably should have known that the creation, distribution, dissemination, or reproduction of the deep fake would cause physical, emotional, reputational, or economic harm to an individual falsely depicted.”²⁹ Second, the Deep Fake must realistically depict either: (1) “[t]he intimate parts of the depicted

individual[;]” or (2) “[t]he depicted individual engaging in a sexual act.”³⁰ Third, the depicted individual must be identifiable “[f]rom the deep fake itself, by the depicted individual or by a reasonable individual viewing or listening to the deep fake[;]”³¹ or “[f]rom the personal information displayed in connection with the deep fake.”³²

The Act also creates a felony criminal offense and penalties for those who “intentionally create or disseminate a deep fake”³³ if certain aggravating factors are present. A perpetrator convicted of a felony under the Act faces up to three years imprisonment, a fine of not more than \$5,000.00, or both, if *any* of the following are true: (1) the depicted individual suffers financial loss;³⁴ (2) the perpetrator created or distributed the Deep Fake with the intent to profit from it;³⁵ (3) the perpetrator maintains an “internet website, online service, online application, or mobile application for the purpose of creating or disseminating the deep fake[;]”³⁶ (4) the perpetrator posts the Deep Fake on a website;³⁷ (5) the perpetrator created the Deep Fake with the intent to “harass, extort, threaten, or cause physical, emotional, reputational, or economic harm to the depicted individual[;]”³⁸ or (6) the perpetrator has previously been convicted for violating MCL 752.388(1).³⁹

For action filed asserting a criminal cause of action under the Act, it is not a defense under MCL 752.388 to assert the individual depicted in the Deep Fake consented to the creation or possession of the Deep Fake, or to the voluntary transmission of the Deep Fake, whether transmitted publicly or privately, unless *both* of the following circumstances apply: (1) the consent is contained in

a written agreement utilizing plain language and executed knowingly and voluntarily by the depicted individual; and (2) the consent documentation includes a general description of the intimate digital depiction of the impacted individual and, if applicable, the audiovisual content into which it will be incorporated.⁴⁰

Moreover, the Act contains an exception which states that MCL 752.388 does not apply if any of the following are relevant to the creation or dissemination of the Deep Fake: (1) the Deep Fake is made for the purpose of a criminal investigation or prosecution; (2) the Deep Fake is for the purpose of, or in connection with, the reporting of conduct that is unlawful; (3) the Deep Fake is made in the course of seeking or receiving medical or mental health treatment, and the Deep Fake work is protected from further dissemination; (4) the Deep Fake relates to a matter of public interest, and the creation or dissemination of the Deep Fake serves a lawful public purpose; or (5) the Deep Fake is made for legal proceedings and is consistent with common practice in civil proceedings necessary for the proper functioning of the civil justice system, or protected by a court order that prohibits any further dissemination of the Deep Fake.⁴¹

The Act provides that MCL 752.388 must not be construed as to impose liability on any of the following entities for providing the infrastructure or access necessary to transmit Deep Fake content created by another person: (1) “[a]n interactive computer service as defined in 47 USC 230(f)(2); (2) “[a] provider of public mobile services or private radio services”; (3) “[a] telecommunications network or broadband provider”; or

(4) “[a] provider or developer of a technology used in the creation of a deep fake, if the technology is not designed for, marketed for, or deployed for the nonconsensual creation or dissemination of deep fakes that realistically depict the intimate parts of depicted individuals or depicted individuals engaging in sexual acts, and if the provider or developer has prohibited explicit deep fake content in accordance with the provider’s or developer’s terms of service.”⁴²

In sum, the same liability carveouts for civil actions brought under the Act are also available as to any criminal charges associated with the creation and dissemination of Deep Fakes under Michigan law.⁴³

The Federal TAKE IT DOWN Act

In May 2025, President Donald J. Trump signed into law the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (the “TAKE IT DOWN Act”) with bipartisan support.⁴⁴ The TAKE IT DOWN Act makes several significant amendments to 47 USC § 223 and 47 USC § 223a, such as:

- Criminalizing the publication of non-consensual intimate visual depictions, which includes both authentic images and AI-generated Deep Fakes.⁴⁵ Penalties for a knowing violation involving an adult can include fines and up to two years of imprisonment.⁴⁶ Publications concerning minors have more stringent requirements and carry a sentence of up to three years.⁴⁷
- Requiring a notice and takedown process for “covered platforms”, including social media websites and mobile applications.⁴⁸ Upon

receiving a valid removal request from an identifiable individual, platforms must remove the intimate visual depiction or deepfake within 48 hours.⁴⁹ The new takedown requirements for platforms are scheduled to take effect on May 19, 2026.⁵⁰

- Holding platforms accountable for non-compliance, with enforcement handled by the Federal Trade Commission (FTC).⁵¹ Failure to reasonably comply with the notice and removal requirements is treated as a violation of the Federal Trade Commission Act.⁵²
- Granting liability protection for good-faith removals.⁵³ Platforms that disable access to or remove content in good faith based on a valid takedown request are protected from legal claims, even if the content is later determined to be lawful.⁵⁴
- Providing definitions for key terms, such as “digital forgery” and “intimate visual depiction”.⁵⁵ For example, a “digital forgery” must be indistinguishable from an authentic visual depiction according to a reasonable person.⁵⁶
- Criminalizing threats to publish intimate visual depictions or Deep Fakes.⁵⁷ The penalties for threats are slightly different, with up to 18 months of imprisonment for threats involving adults and up to 30 months for threats involving minors.⁵⁸

Altogether, the TAKE IT DOWN Act represents a robust federal response to the evolving challenges posed by non-consensual intimate Deep Fakes and related digital forgeries.

By establishing criminal penalties, expedited removal requirements, and platform accountability, the TAKE IT DOWN Act seeks to balance the urgent need for individual privacy and safety with protections for good-faith compliance by technology providers. As these provisions come into force, they are likely to shape both the conduct of online platforms and the legal landscape for victims and content creators alike. However, given the sweeping nature of these reforms, the TAKE IT DOWN Act is expected to face constitutional scrutiny, particularly with respect to the First Amendment and due process concerns.

Constitutional Challenges to Michigan's Protection from Intimate Deep Fakes Act and Federal TAKE IT DOWN Act

As of September 2025, no formal constitutional challenges to the Act have been brought in the state of Michigan, nor challenges to the TAKE IT DOWN Act at the federal level. Nonetheless, commentators across the nation widely anticipate that free speech challenges may be filed against legislation with the same aims as the TAKE IT DOWN Act. In particular, the Electronic Frontier Foundation and Center for Democracy & Technology joined ten other organizations in February of 2025 to oppose the TAKE IT DOWN Act when it was in its bill stage by sending a letter to the Senate which stated, "In its current form, the bill [now, the TAKE IT DOWN Act] creates a notice and takedown (NTD) mechanism that would result in the removal of not just nonconsensual intimate imagery but also speech that is neither illegal nor actually [non-consensual distribution of intimate imagery]. This mechanism is likely unconstitutional and will



undoubtedly have a censorious impact on users' free expression."⁵⁹ Moreover, after its enactment, the Cyber Civil Rights Initiative ("CCRI") issued a statement on April 28, 2025 that said as follows: "CCRI has serious concerns about the constitutionality, efficacy, and potential misuse of TAKE IT DOWN Act's notice and removal provision. While we wholeheartedly support the expeditious removal of nonconsensual intimate content and have long called for increased legal accountability for tech platforms that choose to distribute unlawful content, CCRI objects to the notice and removal provision because it is (1) unlikely to

accomplish these goals and (2) likely to be selectively and improperly misused for political or ideological purposes that endanger the very communities most affected by image-based sexual abuse. CCRI repeatedly raised its concerns about the notice and removal provision with federal lawmakers in the hopes that significant revisions would be made to the bill prior to passage. While some of our suggested revisions were made, the takedown provision as passed by Congress today remains unconstitutionally vague, unconstitutionally overbroad, and lacking adequate safeguards against misuse."⁶⁰

At the state level, though Michigan's Act has yet to face any legal challenges, other states that passed similar legislation to the Act have already encountered scrutiny. For example, on August 5, 2025, a federal judge struck down California's Deep Fake law aimed at restricting AI-generated Deep Fake content during election periods.⁶¹ California's legislation, AB 2655 (officially titled, the Defending Democracy from Deepfake Deception Act of 2024).⁶² Elon Musk's social media platform, X, sued the state of California last year challenging AB 2655.⁶³ Notably, the federal judge – John Mendez – declined to give an opinion on the free speech arguments that were central to the plaintiffs' case within his decision, instead citing the Communications Decency Act of 1996 for online platforms like X as the basis that supported his decision.⁶⁴

Though California's Defending Democracy from Deepfake Deception Act of 2024 was tailored to the use of *political* Deep Fakes, Minnesota, like Michigan, has also developed legislation aimed at creating a broader cause of action for the non-consensual dissemination of Deep Fakes depicting intimate parts or sexual acts of a person within Minnesota Statutes, Chapter 604.⁶⁵

Conclusions

Michigan has joined the likes of Minnesota, Texas, Virginia, California, and others in addressing the proliferation of Deep Fakes. At the federal level, the TAKE IT DOWN Act has similar aims, seeking to set a national standard for platform accountability and victim protections against Deep Fakes. As legislative and judicial

landscapes continue to evolve, ongoing debates around privacy, free speech, and technological innovation will undoubtedly shape the future of this legislation as a whole. The legal and societal response to Deep Fakes remains in flux, with further court challenges, amendments, and stakeholder dialogues likely on the horizon. Ultimately, the effectiveness and fairness of these measures will depend on their ability to protect individuals from harm while safeguarding constitutional rights in the ever-evolving digital age.

Endnotes

1. "Deep Fakes" may also be referred to as deepfakes or deep fakes.
2. MCL 752.381, *et seq.*
3. Available at <https://www.legislature.mi.gov/documents/2025-2026/publicact/pdf/2025-PA-0011.pdf> (last accessed September 3, 2025) and <https://legislature.mi.gov/documents/mcl/pdf/MCL-ACT-11-OF-2025.pdf> (last accessed September 3, 2025).
4. *Science & Tech Spotlight: Deepfakes*, GAO, Publication No. GAO-20-379SP, <https://www.gao.gov/assets/gao-20-379sp.pdf> (last accessed September 3, 2025).
5. *What the heck is a deepfake?*, UNIVERSITY OF VIRGINIA, <https://security.virginia.edu/deepfakes> (last accessed September 3, 2025).
6. *Deepfake technology: What is it, how does it work, and what can it be used for?*, CBBC, <https://www.bbc.co.uk/newsround/69009887> (last accessed September 3, 2025).
7. *What are deepfakes?*, MALWAREBYTES, <https://www.malwarebytes.com/cybersecurity/basics/deepfakes> (last accessed September 3, 2025).
8. MCL 752.381, *et seq.*
9. MCL 752.382(a)(i)-(ii).
10. MCL 752.383.
11. MCL 752.383(a)-(c).
12. MCL 752.384(1).
13. MCL 752.384(2)(a)-(b).
14. MCL 752.384(3).
15. MCL 752.385(1)(a)-(b).
16. MCL 752.385(2)(a).
17. MCL 752.385(2)(b).
18. MCL 752.385(2)(c).
19. MCL 752.385(2)(d).
20. MCL 752.385(2)(e).
21. MCL 752.387(1)(a).
22. MCL 752.387(1)(b).
23. MCL 752.387(1)(c).
24. MCL 752.387(1)(d).
25. MCL 752.386(1)(a).
26. MCL 752.386(1)(b).
27. MCL 752.386(1)(c).
28. MCL 752.388(2).
29. MCL 752.388(1)(a).
30. MCL 752.388(1)(b)(i)-(ii).
31. MCL 752.388(1)(c)(i).
32. MCL 752.388(1)(c)(ii).
33. MCL 752.388 *et seq.*
34. MCL 752.388(3)(a).
35. MCL 752.388(3)(b).
36. MCL 752.388(3)(c).
37. MCL 752.388(3)(d).
38. MCL 752.388(3)(e).
39. MCL 752.388(3)(f).
40. MCL 752.388(4)(a)-(b).
41. MCL 752.388(5)(a)-(e).
42. MCL 752.388(6)(a)-(d).
43. MCL 752.388(5)(a)-(e); MCL 752.388(6)(a)-(d); MCL 752.385(2)(a)-(e); MCL 752.387(1)-(2).
44. Available at <https://www.congress.gov/119/plaws/publ12/PLAW-119publ12.pdf> (last accessed September 3, 2025).
45. 47 U.S. Code § 223(h)(1)-(3).
46. 47 U.S. Code § 223(h)(4)(A).
47. 47 U.S. Code § 223(h)(4)(B).
48. 47 U.S. Code § 223a(a).
49. 47 U.S. Code § 223a(a)(3).
50. *The TAKE IT DOWN Act: A Federal Law Prohibiting the Nonconsensual Publication of Intimate Images*, CONGRESS.GOV, <https://www.congress.gov/crs-product/LSB11314> (last accessed September 4, 2025).
51. 47 U.S. Code § 223a(b).
52. 47 U.S. Code § 223a(b)(1).
53. 47 U.S. Code § 223a(a)(4).
54. *Id.*
55. U.S. Code § 223(h)(1)(B); U.S. Code § 223(h)(1)(E).
56. U.S. Code § 223(h)(1)(B).
57. 47 U.S. Code § 223(h)(6)(A).
58. 47 U.S. Code § 223(h)(6)(B)(i)-(ii).
59. Center for Democracy & Technology et al., *Concerns Regarding the TAKE IT DOWN Act*, CENTER FOR DEMOCRACY & TECHNOLOGY, February 12, 2025, https://cdt.org/wp-content/uploads/2025/02/TAKE-IT-DOWN-Sign-On-Letter_21225.pdf (last accessed September 4, 2025).
60. *CCRI Statement on the Passage of the*

TAKE IT DOWN Act (S. 146), CYBER CIVIL RIGHTS INITIATIVE, April 28, 2025, <https://cybercivilrights.org/ccri-statement-on-the-passage-of-the-take-it-down-act-s-146/> (last accessed September 4, 2025).

61. *Federal Judge Strikes Down California Deepfake Law*, THE CONFERENCE BOARD, August 7, 2025, <https://www.conference-board.org/publications/pdf/index.cfm?brandingURL=federal-judge-strikes-down-california-deepfake-law> (last accessed September 4, 2025).

62. *Id.*

63. *Id.*

64. *Id.*; Chase Difeliciantonio, *Elon Musk and X notch court win against California deepfake law*, POLITICO, August 5, 2025, <https://www.politico.com/news/2025/08/05/elon-musk-x-court-win-california-deepfake-law-00494936> (last accessed September 4, 2025).

65. Minnesota Statutes § 604.32.

Sponsorship Opportunities 25-26

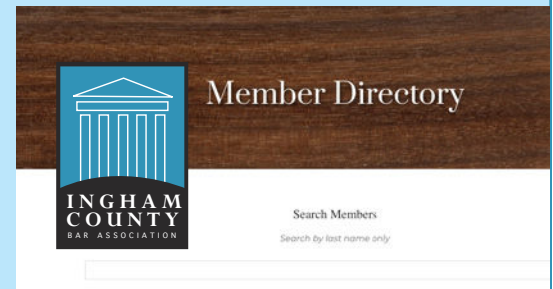
Click here for more information

ICBA MEMBER DIRECTORY

Are you listed in the [online member directory](#)?

Hon. Shauna Dunnings tells why you should be an ICBA Member

CLICK HERE



BRIEFS Author Guidelines & Policies

IN GENERAL

Publication Schedule

Copy Deadline

BRIEFS Committee Meetings

Author and Article Pictures

Article Length and Format

- **Raising the Bar announcements:** 100-200 words
- **Local legal events notices:** 100-150 words
- **Columns:** 300-500 words
- **Articles:** 700-1,000 words
- Submit articles in a Word .doc/.docx

Article Ideas

Opinion Articles

Author Information

INSERT RATES

ARCHIVED ISSUES

BRIEFS Insert Contract, Rates & Policies