

Artificial Intelligence (AI)

Interim Guidance

June 2024

from the AI Rapid Response Team at the National Center for State Courts

AI and the Courts: Digital Evidence and Deepfakes in the Age of AI

AI advances are causing challenges in the courtroom as judges grapple with evidentiary issues related to digitally enhanced evidence as well as the emergence of deepfakes (convincing false pictures, videos, audio, and other digital information). These advances make it easier and cheaper to enhance digital evidence or create deepfakes causing evidentiary issues to arise.

Digitally Enhanced Evidence

Digitally enhanced evidence is audio, videos, or images that have been enhanced by AI software. The purpose is generally to improve the quality of audio, videos, or images. This differs from past uses, such as zooming in on an image, speeding up or slowing down a video, or separating a voice from background noise, in that AI may fill in pixels on the image with what the software thinks should be in the image, thus altering it from the original.

This technology was recently at the center of a criminal trial in Washington state when digitally enhanced video was not admitted into evidence. The court based its decision on the testimony of the expert witness who testified “the AI tool(s) utilized ... added approximately sixteen times the number of pixels, compared to the number of pixels in the original images to enhance each video frame, utilizing an algorithm and enhancement method unknown to and unreviewed by any forensic video expert.” The court found that the expert “demonstrated that the AI method created false image detail and that process is not acceptable to the forensic video community because it has the effect of changing the meaning of portions of the video.”

It may be necessary for courts to consider changes to the rules of evidence but until that happens, Judges may need to require expert testimony to determine the authenticity and reliability of audio, videos, and images that are challenged rather than relying on the standards for admission.

What is a Deepfake?

“Deepfake” refers to fabricated or altered but realistic audio, videos, or images made using software, for example, by embedding another person’s likeness into an image or video. Deepfakes have become very sophisticated in recent years, and it is not easy for an average person to identify the audio, video, or image as fake.

Deepfakes and the Courts

The issue of deepfakes can arise in any court proceeding in which a party presents digital evidence in the form of an image, video, or audio. Fabricated evidence could be submitted as authentic evidence or authentic evidence could be challenged as fabricated evidence. When a party alleges that digital evidence has been fabricated, expert testimony may be needed to authenticate the challenged evidence. This could result in a battle between the experts and higher litigation costs for all parties and could widen the access to justice gap.¹

¹ Delfino, Rebecca, Pay-to-play: Access to Justice in the Era of AI and Deepfakes (February 10, 2024). Loyola Law School, Los Angeles Legal Studies Research Paper No. 2024-08.

Of concern is the effect that deepfakes could have on the case's outcome because of the considerable impact that visual evidence has on fact finders. According to studies referenced in a recent law journal article, as compared to jurors who hear just oral testimony, "jurors who hear oral testimony along with video testimony are 650% more likely to retain the information."² Once jurors have seen video evidence, it is very hard for the impact to be undone, even with admonishments to the jury. Another study published in 2021 by the Center for Humans and Machines at the Max Planck Institute for Human Development and the University of Amsterdam School of Economics, demonstrates the difficulty of identifying deepfakes. The study found that the participants could not reliably detect deepfakes. The study found that people are biased towards identifying deepfakes as authentic (not vice versa) and overestimate their own abilities to detect deepfakes even after being instructed on how to detect deepfakes.³ The mere existence of deepfakes combined with proliferation of online information, both real and fabricated, that people are exposed to daily may also lead to jury skepticism because people do not know what information they can trust.⁴

Current Evidentiary Rules

The existing Federal Rules of Evidence and the various state rules of evidence require that any evidence submitted must be real and that the party submitting the evidence has the obligation to authenticate it, by proving that the evidence is what it purports to be. Judicial officers already have an obligation to determine whether the probative value of the evidence submitted outweighs the possible unfair prejudice, confusion of the issues, or misleading of the jury that would result from its admission.

Are the Current Rules Sufficient?

Prior to the advent of deepfakes, the rules of evidence have been sufficient to adapt to technology changes. Laws and rules of evidence addressing deepfakes lag behind the technology. At present, tools to detect deepfakes are not as sophisticated as the tools to create deepfakes such that not all deepfakes will be identifiable. To mitigate the impact of deepfakes on litigation and jurors, judicial officers should identify related evidentiary issues and rule on those prior to trial and outside the presence of the jury, if possible.

The legal community is having ongoing discussions about the need for changes to the rules of evidence. However, it will be important for the courts to address the potential for harm to the legal process that deepfakes pose, and to evaluate whether more stringent rules should be adopted for the admission of digital evidence. In addition, for case types with high rates of self-representation, relying on the parties to challenge the authentication of evidence, which the current adversarial process requires, may be unrealistic. If deepfakes proliferate, courts may need to reconsider who is responsible for determining whether evidence is authentic, especially if reliable technology tools become available that would enable courts to determine if something is real or fake. If deepfakes become ubiquitous, the perception may shift to believing every piece of evidence is fake or has been altered; if so, this may require a more arduous authentication process routinely involving experts, costs, new technologies, elongating the length of trials. This would be a significant shift from current practices.

² Rebecca A. Delfino, *Deepfakes on Trial: A Call To Expand the Trial Judge's Gatekeeping Role To Protect Legal Proceedings from Technological Fakery*, 74 HASTINGS L.J. 293 (2023).

³ Köbis NC, Doležalová B, Soraperra I. *Foiled twice: People cannot detect deepfakes but think they can*. *iScience*. 2021 Oct 29;24(11):103364. doi: 10.1016/j.isci.2021.103364. PMID: 34820608; PMCID: PMC8602050.

⁴ Rebecca A. Delfino, *Deepfakes on Trial: A Call To Expand the Trial Judge's Gatekeeping Role To Protect Legal Proceedings from Technological Fakery*, 74 HASTINGS L.J. 293 (2023).

1 DAVID CHIU, SBN 189542
City Attorney
2 YVONNE R. MERÉ, SBN 173594
Chief Deputy City Attorney
3 SARA J. EISENBERG, SBN 269303
Chief of Complex and Affirmative Litigation
4 RONALD H. LEE, SBN 238720
Assistant Chief of Complex and Affirmative Litigation
5 KARUN A. TILAK, SBN 323939
MIGUEL A. GRADILLA, SBN 304125
6 DAVID S. LOUK, SBN 304654
Deputy City Attorneys
7 Fox Plaza
1390 Market Street, 6th Floor
8 San Francisco, CA 94102-5408
Telephone: (415) 355-3308 (Tilak)
9 (415) 554-3870 (Gradilla)
(415) 355-3314 (Louk)
10 Facsimile: (415) 437-4644
E-Mail: Karun.Tilak@sfcityatty.org
11 Miguel.Gradilla@sfcityatty.org
David.Louk@sfcityatty.org
12

Attorneys for Plaintiff

13 PEOPLE OF THE STATE OF CALIFORNIA, acting by
and through San Francisco City Attorney DAVID CHIU
14

15 SUPERIOR COURT OF THE STATE OF CALIFORNIA

16 COUNTY OF SAN FRANCISCO

17 UNLIMITED JURISDICTION

18 PEOPLE OF THE STATE OF CALIFORNIA,
19 acting by and through San Francisco City
Attorney DAVID CHIU,

20 Plaintiff,

21 vs.

22 SOL ECOM, INC., BRIVER LLC, ITAI
23 TECH LTD., DEFIREX OÜ, ITAI OÜ,
24 AUGUSTIN GRIBINETS, and DOES #1
through #50,

25 Defendants.
26
27
28

Case No. CGC-24-617237

**FIRST AMENDED COMPLAINT FOR
INJUNCTIVE RELIEF AND CIVIL
PENALTIES FOR VIOLATIONS OF
BUSINESS AND PROFESSIONS CODE
SECTION 17200**

ELECTRONICALLY
FILED
Superior Court of California,
County of San Francisco

08/16/2024
Clerk of the Court
BY: JAMES FORONDA
Deputy Clerk

1 Plaintiff, the People of the State of California (the “People”), acting by and through San
2 Francisco City Attorney David Chiu, brings this action against Sol Ecom, Inc., Briver LLC, Itai Tech
3 Ltd., Defirex OÜ, Itai OÜ, Augustin Gribinets, and Does #1 through #50 (together, the “Defendants”),
4 and alleges as follows:

5 INTRODUCTION

6 1. Rapid advancements in the field of artificial intelligence (“AI”) in recent years have
7 created immense opportunities for innovation, with major implications for scientific research,
8 healthcare, education, computing, and beyond.

9 2. Among the most significant developments is the emergence of generative AI models
10 that have the capacity to create content, be it in the form of text, speech, images, video, or music.

11 3. Despite the potential for generative AI models to improve people’s lives, they also
12 present new and profound safety and privacy concerns. In particular, some generative AI models have
13 been released to the public as open source with the goal of fostering innovation and collaboration, but
14 have been adapted and misused for illegal and harmful purposes.

15 4. One disturbing form of misuse is the adaptation of open-source AI image generation
16 models to create fake pornographic and sexual abuse content depicting real, identifiable women and
17 girls, so-called “deepfake pornography” or “deepnudes.”

18 5. These models have led to the proliferation of websites and apps that offer to “undress”
19 or “nudify” women and girls. By exploiting open-source AI image generation models, these websites
20 and apps manipulate images of real women and girls without their consent to create photorealistic
21 images showing these women and girls with AI-generated nude bodies and intimate body parts.

22 6. Defendants operate some of the world’s most popular websites that offer to nudify
23 images of women and girls. The primary purpose of Defendants’ websites is to create fake, nude
24 images of women and girls without their consent. Defendants tout their ability to let users “see anyone
25 naked.” As one Defendant puts it: “[i]magine wasting time taking her out on dates, when you can just
26 use [the website] to get her nudes.” Collectively, these sites have been visited over 200 million times
27 just in the first six months of 2024.

1 7. Nonconsensual intimate images (“NCII”) generated from Defendants’ websites—and
2 other similar websites—are used to bully, threaten, and humiliate women and girls.¹ In California and
3 across the country, there has been a stark increase in the number of women and girls harassed and
4 victimized by AI-generated NCII, and this distressing trend shows no sign of abating. For example, in
5 February 2024, AI-generated nude images of sixteen eighth-grade students were circulated among
6 students at a California middle school.² Reports of the use of AI-generated NCII to target and bully
7 schoolchildren—primarily girls—in California and across the country abound.³ The Federal Bureau
8 of Investigation has also warned of an uptick in instances of extortion schemes where bad actors use
9 public social media pictures of their victims to create AI-generated nude and sexually explicit images
10 and threaten to release the images if the victims do not pay them.⁴

12 ¹ Coralie Kraft, *Trolls Used Her Face to Make Fake Porn. There Was Nothing She Could Do*,
13 The New York Times Magazine (July 31, 2024), <https://www.nytimes.com/2024/07/31/magazine/sabrina-javellana-florida-politics-ai-porn.html> (archived at <https://perma.cc/5XNQ-22RB>).

14 ² Jon Healey, *Beverly Hills School District Expels 8th Graders Involved In Fake Nude Scandal*,
15 Los Angeles Times (Mar. 7, 2024), <https://www.latimes.com/california/story/2024-03-07/beverly-hills-school-district-expels-8th-graders-involved-in-fake-nude-scandal> (archived at <https://perma.cc/57AT-NMXE>).

16 ³ Howard Blume, *L.A. School District Probes Inappropriate Images Shared at Fairfax High. More AI Abuse?*,
17 Los Angeles Times (Apr. 9, 2024), <https://www.latimes.com/california/story/2024-04-09/student-generated-inappropriate-ai-image-of-girls-at-fairfax-high> (archived at <https://perma.cc/B8CK-68E6>); Bridget Chavez, *No Charges as AI-Generated Nude Pictures of Female Students Circulate Around Issaquah School*,
18 KIRO7.com (Nov. 9, 2023), <https://www.kiro7.com/news/local/no-charges-ai-generated-nude-pictures-female-students-circulate-around-issaquah-school/MCQTOKWRVREPTK3K2IAQWTRR6U/> (archived at <https://perma.cc/84CJ-WQXL>);
19 Hannah Fry, *Laguna Beach High School Investigates ‘Inappropriate’ AI-generated Images of Students*,
20 Los Angeles Times (Apr. 2, 2024), <https://www.latimes.com/california/story/2024-04-02/laguna-beach-high-school-investigating-creation-of-ai-generated-images-of-students> (archived at
21 <https://perma.cc/S4EG-KUY7>); Josh Haskell, *Calabasas Teen Says Classmate Not Disciplined For Sharing Real and Fake Nude Images of Her*,
22 ABC7.com (Mar. 14, 2024), <https://abc7.com/calabasas-high-school-student-accuses-classmate-sharing-real-and-fake-nude-photos/14521422/> (archived at
23 <https://perma.cc/S68X-8V9B>); Anthony Johnson, *Call for Action at Westfield High School After AI Used to Make Fake Pornographic Images of Girls*,
24 ABC7NY.com (Nov. 3, 2023), <https://abc7ny.com/nj-westfield-high-school-artificial-intelligence-pornographic-images/14009286/>
25 (archived at <https://perma.cc/G9XZ-4D3G>); Liz Landers et al., *A 15-year-old’s Prom Picture was Altered into AI-created Nudes*,
26 Scripps News (May 22, 2024), <https://www.scrippsnews.com/politics/disinformation-desk/high-schools-nationwide-are-facing-a-new-problem-ai-generated-nudes> (archived at
27 <https://perma.cc/HSV8-X56K>).

28 ⁴ James Vincent, *Blackmailers are Using Deepfaked Nudes to Bully and Extort Victims, Warns FBI*,
The Verge (June 8, 2023), <https://www.theverge.com/2023/6/8/23753605/ai-deepfake-sextortion-nude-blackmail-fbi-warning> (archived at <https://perma.cc/9E4N-DDHX>).

1 8. Victims have little to no recourse, as they face significant obstacles to remove these
2 images once they have been disseminated. They are left with profound psychological, emotional,
3 economic, and reputational harms, and without control and autonomy over their bodies and images.
4 As one victim explained, “I felt like I didn’t have a choice in what happened to me or what happened
5 to my body.”⁵ Another emphasized that she and her family live in “hopelessness and perpetual fear
6 that, at any time, such images can reappear and be viewed by countless others.”⁶

7 9. Given the widespread availability and popularity of Defendants’ websites, San
8 Franciscans and Californians face the threat that they or their loved ones may be victimized in this
9 manner.

10 10. Defendants’ conduct violates state and federal laws prohibiting the creation, possession,
11 disclosure, and distribution of AI-generated NCII and similar forms of sexual abuse and harassment.

12 11. The People bring this case to hold Defendants accountable for creating and distributing
13 AI-generated NCII of women and girls and for aiding and abetting others in perpetrating this conduct.

14 **PARTIES**

15 12. Plaintiff, the People of the State of California, acting by and through San Francisco
16 City Attorney David Chiu, prosecutes this action pursuant to Business and Professions Code section
17 17200 *et seq.*

18 13. Defendant Sol Ecom, Inc. (“Sol Ecom”) is a corporation organized under the laws of
19 the state of Florida with its principal place of business at 610 South Main Street, Apartment 730, Los
20 Angeles, California, 90014. Sol Ecom owns and operates the website [REDACTED] which produces
21 AI-generated NCII of adults.

22 14. Defendant Briver LLC (“Briver”) is a corporation organized under the laws of the state
23 of New Mexico with its principal place of business at 530-B Harkle Road, Suite 100, Santa Fe, New
24

25
26 ⁵ Coralie Kraft, *supra* n.1.

27 ⁶ Charles Toutant, *An AI Took Her Clothes Off. Now a New Lawsuit Will Test Rules for*
28 *Deepfake Porn*, Law.com (Feb. 5, 2024), <https://www.law.com/njlawjournal/2024/02/05/an-ai-took-her-clothes-off-now-a-new-lawsuit-will-test-rules-for-deepfake-porn/?sreturn=20240704180530>,
(archived at <https://perma.cc/7ENN-Y6VH>).

1 Mexico 87505. Briver owns and operates the websites [REDACTED] and [REDACTED], which produce
2 AI-generated NCII of adults and children.

3 15. Defendant Itai Tech Ltd. (“Itai Tech”) is a corporation organized under the laws of the
4 United Kingdom with its registered office address at 81 Anthony Drive, Norwich, England, United
5 Kingdom, NR3 4EW. Itai Tech owns and operates the websites [REDACTED], [REDACTED],
6 [REDACTED], and [REDACTED]. The website [REDACTED] produces AI-generated NCII of adults. The
7 website [REDACTED] produces AI-generated NCII of adults and children. On information and belief,
8 the websites [REDACTED] and [REDACTED] produce AI-generated NCII of adults.

9 16. Defendant Defirex OÜ (“Defirex”) is a corporation organized under the laws of Estonia
10 with a registered address at Vesivärava tn 50-301, Kesklinna linnaosa, 10152 Tallinn and a contact
11 address at Väike-Paala tn 2, Lasnamäe linnaosa, 11415 Tallinn. Defirex owns and operates the
12 website [REDACTED]. On information and belief, [REDACTED] produces AI-generated NCII of
13 adults.

14 17. Defendant Itai OÜ is a corporation organized under the laws of Estonia with a contact
15 address of Järvevana tee 9, Kesklinna linnaosa, 11314 Tallinn. Itai OÜ has a registered address of
16 Branka Bajića 9e, Novi Sad, Serbia. Itai OÜ owns and operates the website [REDACTED], which
17 produces AI-generated NCII of adults.

18 18. Defendant Augustin Gribinets (“Gribinets”) is a resident of Estonia. Gribinets owns
19 and operates the website [REDACTED], which produces AI-generated NCII of adults and children.

20 19. Defendant Doe #1 owns and operates the website [REDACTED], which produces AI-
21 generated NCII of adults and children. The People are not currently aware of the true identity of Doe
22 #1, and therefore sue this Defendant under a fictitious name. The People will seek leave to amend this
23 complaint to allege Doe #1’s true identity when that information is ascertained.

24 20. Defendant Doe #2 owns and operates the websites [REDACTED] and [REDACTED], which
25 produce AI-generated NCII of adults and children. The People are not currently aware of the true
26 identity of Doe #2, and therefore sue this Defendant under a fictitious name. The People will seek
27 leave to amend this complaint to allege Doe #2’s true identity when that information is ascertained.
28

1 21. Defendant Doe #3 owns and operates the website [REDACTED] which produces AI-
2 generated NCII of adults and children. The People are not currently aware of the true identity of Doe
3 #3, and therefore sue this Defendant under a fictitious name. The People will seek leave to amend this
4 complaint to allege Doe #3's true identity when that information is ascertained.

5 22. Defendant Doe #4 owns and operates the website [REDACTED], which produces AI-
6 generated NCII of adults and children. The People are not currently aware of the true identity of Doe
7 #4, and therefore sue this Defendant under a fictitious name. The People will seek leave to amend this
8 complaint to allege Doe #4's true identity when that information is ascertained.

9 23. Defendant Doe #5 owns and operates the website [REDACTED], which produces AI-
10 generated NCII of adults. The People are not currently aware of the true identity of Doe #5, and
11 therefore sue this Defendant under a fictitious name. The People will seek leave to amend this
12 complaint to allege Doe #5's true identity when that information is ascertained.

13 24. The People are not aware of the true names and capacities of Defendants sued as Does
14 #6 through #50, inclusive, and therefore sue these Defendants by such fictitious names. Each
15 fictitiously named Defendant is responsible in some manner for the violations of law alleged. The
16 People will seek leave to amend this complaint to allege their true names and capacities when that
17 information is ascertained.

18 25. Whenever this Complaint refers to "Defendants," such reference shall include Does 1
19 through 50 as well as the named Defendants.

20 26. Whenever this complaint refers to any act of any corporate defendant, such allegation
21 shall be deemed to mean that such corporate defendant did the acts alleged in the complaint through its
22 officers, directors, agents, employees, and/or representatives while they were acting within the actual
23 or ostensible scope of their authority.

24 27. On information and belief, each Defendant owns and operates other websites that
25 produce AI-generated NCII of adults and/or children. The People will seek leave to amend this
26 complaint to identify these additional websites when that information is ascertained.

1 **JURISDICTION AND VENUE**

2 28. The San Francisco Superior Court has jurisdiction over this action. Upon information
3 and belief, Defendants are engaging in unlawful and unfair business practices in San Francisco, and
4 the San Francisco City Attorney has statutory authority to prosecute this case on behalf of the People.

5 29. Venue is proper in this Court because, upon information and belief, the unlawful
6 conduct occurred in San Francisco and elsewhere in California.

7 **FACTUAL ALLEGATIONS**

8 **I. The Development and Misuse of Open-Source AI Image Generation Models**

9 30. Among the most significant recent developments in AI is the advent of highly
10 sophisticated generative AI models. While the specific computing techniques used in these models
11 differ, in general these models are fed vast quantities of data and are trained to detect patterns and
12 generate new content that mimics the information they have ingested.

13 31. Several companies have deployed this technology to develop AI models specifically
14 designed to generate images or edit existing images based on text prompts from users. These models
15 are trained on enormous datasets consisting of hundreds of millions of images and associated text from
16 the Internet, and learn to recognize features of these images and the text descriptions associated with
17 such features.

18 32. Several such models are made available to the public as “open-source” models. With
19 an open-source model, any member of the public can adapt and train a specific implementation of that
20 model on additional images in order to hone (or “fine tune”) its ability to generate specific kinds of
21 content. These models can be modified and adapted by anyone for almost any purpose.
22 Consequently, these open-source models have been adapted and trained to create new fine-tuned
23 versions that are highly effective at generating pornographic content.⁷ Even where the creators of
24 these open-source models subsequently incorporate safeguards into new releases of the model, earlier

25
26 ⁷ Will Knight, *This Uncensored AI Art Tool Can Generate Fantasies—and Nightmares*, Wired
27 (Sept. 21, 2022), <https://www.wired.com/story/the-joy-and-dread-of-ai-image-generators-without-limits/> (archived at <https://perma.cc/7MBU-CHRV>); Lydia Morrish, *The Dark Side of Open Source AI Image Generators*, Wired (Mar. 6, 2024), <https://www.wired.com/story/dark-side-open-source-ai-image-generators/> (archived at <https://perma.cc/CUN9-VHMA>).

1 releases—and fine-tuned versions trained to generate pornographic content—continue to circulate
2 online.

3 33. These highly popular fine-tuned versions generate not only pornographic content
4 involving fictitious AI-generated individuals, but also manipulate images of real people to produce
5 fictional pornographic content that depicts those individuals. The models are able to recognize
6 clothing and body features in an image of a person, and can be further conditioned to manipulate the
7 image to generate a fake, photorealistic image that maintains the person’s face, but replaces their
8 clothed body with a nude body—thus appearing to “undress” the person and display their intimate
9 body parts. These models “undress” or “nudify” not only adults, but also children.

10 34. These manipulated intimate images are generated without the consent of the persons
11 depicted, resulting in the creation and dissemination of AI-generated NCII of these individuals.

12 35. The availability of these fine-tuned versions designed to create AI-generated NCII has
13 spawned the development of websites dedicated to creating “nudified” images of women and girls.⁸
14 These websites offer user-friendly interfaces for uploading clothed images of real people to generate
15 realistic “nudified” versions of those images. These websites require users to subscribe or pay to
16 generate nude images. Some websites give users a “free trial,” allowing them to create a limited
17 number of free images as a way of enticing them to pay for additional images.

18 **II. Defendants Operate Popular Websites Used to Nudify Images of Women and Girls**

19 36. Defendants operate some of the world’s most popular websites specifically designed to
20 generate and distribute AI-generated NCII of women and girls.

21 **Sol Ecom**

22 37. Sol Ecom owns and operates the website [REDACTED]. [REDACTED] had over 12
23 million visits in the first six months of 2024.

24 38. Users can access [REDACTED] by signing in using their Google, Discord, or X
25 accounts.

26
27
28 ⁸ Santiago Lakatos, *A Revealing Picture*, Graphica (Dec. 8, 2023), <https://graphika.com/reports/a-revealing-picture> (archived at <https://perma.cc/5BCN-G4R3>).

1 94. Gribinets intentionally creates and distributes to, or otherwise knowingly encourages,
2 enables, and facilitates the creation and distribution of, AI-generated NCII of identifiable women and
3 girls to users with the knowledge that these images will traumatize and cause severe emotional distress
4 to the depicted individuals if disclosed.

5 **Doe #1**

6 95. Doe #1 owns and operates the website [REDACTED]. [REDACTED] had over 32 million
7 visits in the first six months of 2024.

8 96. Doe #1 promotes [REDACTED] as “the best free AI deepnude nudifier to see anyone
9 naked.”

10 97. Users can access [REDACTED] by signing in using their Google accounts.

11 98. Users can upload an image of a clothed woman to [REDACTED], and the site will create
12 a fake nude image of the subject.

13 99. Because Doe #1 has failed to deploy available technology to detect images of minors,
14 users can upload an image of a clothed girl under 18 years old to [REDACTED], and the site will create
15 a fake nude image of the subject.

16 100. Doe #1 allows users to generate a limited number of nudified images for free, after
17 which users must purchase credits in order to generate additional images. On information and belief,
18 users can purchase credits from Doe #1 using cryptocurrency.

19 101. Doe #1 fails to verify that depicted individuals in the images generated by [REDACTED]
20 have consented to the nudification of their respective images. In fact, Doe #1 promotes the website as
21 a way to see “anyone” naked.

22 102. Doe #1 knows that the primary purpose of websites like [REDACTED] is to create AI-
23 generated NCII of identifiable women and girls.

24 103. Doe #1 intentionally creates and distributes to, or otherwise knowingly encourages,
25 enables, and facilitates the creation and distribution of, AI-generated NCII of identifiable women and
26 girls to users with the knowledge that these images will traumatize and cause severe emotional distress
27 to the depicted individuals if disclosed.

28

1 abetted violations of California Civil Code section 1708.85(a) by their acts and
2 practices set forth herein.

3 c. Defendants have violated California Penal Code section 647(j)(4) prohibiting the
4 intentional distribution of nonconsensual depictions of intimate body parts of an
5 identifiable person, or aided and abetted violations of California Penal section 647(j)(4)
6 in violation of California Penal Code section 31 by the acts and practices set forth
7 herein.

8 d. Defendants have violated 15 U.S.C. § 6851(b)(1) prohibiting the knowing or reckless
9 disclosure in interstate commerce of intimate visual depictions of identifiable persons,
10 or aided and abetted violations of 15 U.S.C. § 6851(b)(1) by the acts and practices set
11 forth herein.

12 148. Defendants have engaged in and continue to engage in unfair business acts and
13 practices in violation of section 17200. Defendants' acts and practices of creating nudified images
14 constitute unfair business practices because they offend established public policy, the harm they cause
15 to consumers greatly outweighs any benefits associated with those practices, and they are immoral,
16 unethical, oppressive, unscrupulous and/or substantially injurious to consumers.

17 **SECOND CAUSE OF ACTION**

18 **VIOLATION OF BUSINESS AND PROFESSIONS CODE 17200**

19 **AGAINST DEFENDANTS BRIVER LLC, ITAI TECH LTD., AUGUSTIN GRIBINETS,**

20 **DOE #1, DOE #2, DOE #3 & DOE #4**

21 149. The People incorporate by reference the allegations contained in each paragraph above,
22 as if those allegations were fully set forth in this cause of action.

23 150. California Business and Professions Code section 17200 prohibits any "unlawful,
24 unfair, or fraudulent business act or practice."

25 151. Defendants Briver LLC, Itai Tech Ltd., Augustin Gribinets, Doe #1, Doe #2, Doe #3,
26 and Doe #4 are engaged in and continue to engage in unlawful business acts and practices in violation
27 of section 17200. Such acts and practices include, but are not limited to, the following:
28

- 1 a. Each of the above-named Defendants has violated California Penal Code section
2 311.3(a) prohibiting the knowing development of nonconsensual obscene images of
3 persons under the age of 18 years, or aided and abetted violations of California Penal
4 section 311.3(a) in violation of California Penal Code section 31 by the acts and
5 practices set forth herein.
- 6 b. Each of the above-named Defendants has violated California Penal Code section
7 311.2(a) prohibiting the knowing distribution of obscene images, or aided and abetted
8 violations of California Penal section 311.2(a) in violation of California Penal Code
9 section 31 by the acts and practices set forth herein.
- 10 c. Each of the above-named Defendants has violated California Penal Code section
11 311.2(b) prohibiting the knowing distribution for commercial gain of obscene images
12 depicting persons under the age of 18 years engaged in sexual conduct, or aided and
13 abetted violations of California Penal section 311.2(b) in violation of California Penal
14 Code section 31 by the acts and practices set forth herein.
- 15 d. Each of the above-named Defendants has violated California Penal Code section
16 311.2(c) prohibiting the knowing distribution to adults of images depicting persons
17 under the age of 18 years engaged in sexual conduct, or aided and abetted violations of
18 California Penal section 311.2(c) in violation of California Penal Code section 31 by
19 the acts and practices set forth herein.
- 20 e. Each of the above-named Defendants has violated 18 U.S.C. § 1465 prohibiting the
21 knowing production of any obscene images with the intent to distribute by interactive
22 computer service, or aided and abetted violations of 18 U.S.C. § 1465 in violation of 18
23 U.S.C. § 2(a) by the acts and practices set forth herein.
- 24 f. Each of the above-named Defendants has violated 18 U.S.C. § 1466 prohibiting
25 engaging in the business of distributing, or knowingly producing with intent to
26 distribute, any obscene images by interactive computer service, or aided and abetted
27 violations of 18 U.S.C. § 1466 in violation of 18 U.S.C. § 2(a) by the acts and practices
28 set forth herein.

- 1 g. Each of the above-named Defendants has violated 18 U.S.C. § 1466A(a)(1) prohibiting
2 the knowing distribution of, or production with intent to distribute, obscene depictions
3 of minors engaging in sexually explicit conduct that were produced by computer, or
4 aided and abetted violations of 18 U.S.C. § 1466A(a)(1) in violation of 18 U.S.C. § 2(a)
5 by the acts and practices set forth herein.
- 6 h. Each of the above-named Defendants has violated 18 U.S.C. § 1466A(b)(1) prohibiting
7 the knowing possession of obscene depictions of minors engaging in sexually explicit
8 conduct that were produced by computer, or aided and abetted violations of 18 U.S.C.
9 § 1466A(b)(1) in violation of 18 U.S.C. § 2(a) by the acts and practices set forth herein.
- 10 i. Each of the above-named Defendants has violated 18 U.S.C. § 2252A(a)(1) prohibiting
11 the knowing distribution of any child pornography by computer, or aided and abetted
12 violations of 18 U.S.C. § 2252A(a)(1) in violation of 18 U.S.C. § 2(a) by the acts and
13 practices set forth herein.
- 14 j. Each of the above-named Defendants has violated 18 U.S.C. § 2252A(a)(2) prohibiting
15 the knowing receipt or distribution of any child pornography or materials containing
16 child pornography by computer, or aided and abetted violations of 18 U.S.C.
17 § 2252A(a)(2) in violation of 18 U.S.C. § 2(a) by the acts and practices set forth herein.
- 18 k. Each of the above-named Defendants has violated 18 U.S.C. § 2252A(a)(4)(B)
19 prohibiting the knowing sale of any child pornography by computer, or aided and
20 abetted violations of 18 U.S.C. § 2252A(a)(4)(B) in violation of 18 U.S.C. § 2(a) by the
21 acts and practices set forth herein.
- 22 l. Each of the above-named Defendants has violated 18 U.S.C. § 2252A(5)(B) prohibiting
23 the knowing possession of child pornography that was produced or distributed by
24 computer, or aided and abetted violations of 18 U.S.C. § 2252A(5)(B) in violation of 18
25 U.S.C. § 2(a) by the acts and practices set forth herein.
- 26 m. Each of the above-named Defendants has violated 18 U.S.C. § 2252A(a)(7) prohibiting
27 the knowing production or distribution of any adapted or modified images of child
28 pornography of identifiable minors by computer, or aided and abetted violations of 18

1 U.S.C. § 2252A(a)(7) in violation of 18 U.S.C. § 2(a) by the acts and practices set forth
2 herein.

3 152. Defendants Briver LLC, Itai Tech Ltd., Augustin Gribinets, Doe #1, Doe #2, Doe #3,
4 and Doe #4 are engaged in and continue to engage in unfair business acts and practices in violation of
5 section 17200. Each of the above-named Defendants' acts and practices of creating nudified images
6 of children constitute unfair business practices because they offend established public policy, the harm
7 they cause to consumers greatly outweighs any benefits associated with those practices, and they are
8 immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers.

9 **PRAYER FOR RELIEF**

10 The People respectfully request that the Court enter judgment in favor of the People and
11 against Defendants, jointly and severally, and grant the following relief:

12 1. Enjoin all Defendants, their successors, agents, representatives, employees, and any and
13 all other persons who act in concert or participation with Defendants by preliminarily and permanently
14 restraining them from performing or proposing to perform any acts in violation of California Business
15 and Professions Code section 17200 as set forth above, including but not limited to ceasing operation
16 of all websites they own or operate that are capable of creating AI-generated NCII of identifiable
17 individuals.

18 2. Order that any domain-name registrars, domain-name registries, webhosts, payment
19 processors, or companies providing user authentication and authorization services or interfaces who
20 are provided with notice of the injunction, shall take all actions necessary to restrain Defendants from
21 performing or proposing to perform any unlawful or unfair business practices in violation of California
22 Business and Professions Code section 17200, including but not limited to ceasing to facilitate access
23 to any websites owned or operated by Defendants that are capable of creating AI-generated NCII of
24 identifiable individuals.

25 3. Order each Defendant to pay a civil penalty of \$2,500 for each violation of California
26 Business and Professions Code section 17200.

27 4. Order Defendants to pay the costs of suit; and
28

1 5. Provide such further and additional relief as the Court deems just, proper, and
2 equitable.

3 Dated: August 16, 2024

4 DAVID CHIU
 City Attorney
5 YVONNE R. MERÉ
 Chief Deputy City Attorney
6 SARA J. EISENBERG
 Chief of Complex and Affirmative Litigation
7 RONALD H. LEE
 Assistant Chief of Complex and Affirmative Litigation
8 KARUN A. TILAK
 MIGUEL A. GRADILLA
9 DAVID S. LOUK
 Deputy City Attorneys

10
11 By: 
12 _____

KARUN A. TILAK

13 *Attorneys for Plaintiff*
14 PEOPLE OF THE STATE OF CALIFORNIA, acting by
15 and through San Francisco City Attorney DAVID CHIU



IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA

SEALED INDICTMENT

v.

Case No. 24-cr-50-jdp
18 U.S.C. § 1466A(a)(1), (b)(1)
18 U.S.C. § 1470

STEVEN ANDEREGG,

Defendant.

THE GRAND JURY CHARGES:

COUNT 1

Between on or about October 20, 2023, and on or about December 28, 2023, in the Western District of Wisconsin, the defendant,

STEVEN ANDEREGG,

knowingly produced at least one visual depiction that depicted a minor engaging in sexually explicit conduct and was obscene, and attempted to do so, and any visual depiction involved in the offense had been shipped and transported in interstate and foreign commerce by any means, including by computer, and was produced using materials that had been mailed, and that had been shipped and transported in interstate and foreign commerce by any means, including by computer.

(In violation of Title 18, United States Code, Section 1466A(a)(1) and (d)(4)).

COUNT 2

On or about October 7, 2023, in the Western District of Wisconsin, the defendant,

STEVEN ANDEREGG,

knowingly distributed at least one visual depiction that depicted a minor engaging in sexually explicit conduct and was obscene, and any communication involved in and made in furtherance of the offense was communicated and transported in interstate and foreign commerce by any means, including by computer, and any means and instrumentality of interstate and foreign commerce was otherwise used in committing and in furtherance of the commission of the offense.

(In violation of Title 18, United States Code, Section 1466A(a)(1) and (d)(1)).

COUNT 3

On or about October 7, 2023, in the Western District of Wisconsin, the defendant,

STEVEN ANDEREGG,

using a facility and means of interstate commerce, knowingly transferred obscene matter to another individual who had not attained the age of 16 years, knowing that such other individual had not attained the age of 16 years, and attempted to do so.

(In violation of Title 18, United States Code, Section 1470).

COUNT 4

From on or about October 20, 2023, to on or about February 22, 2024, in the Western District of Wisconsin, the defendant,

STEVEN ANDEREGG,

knowingly possessed at least one visual depiction that depicted a minor engaging in sexually explicit conduct and was obscene, and any visual depiction involved in the offense had been shipped and transported in interstate and foreign commerce by any means, including by computer, and was produced using materials that had been

mailed, and that had been shipped and transported in interstate and foreign commerce by any means, including by computer.

(In violation of Title 18, United States Code, Section 1466A(b)(1) and (d)(4)).

FORFEITURE ALLEGATION

Upon conviction of any offense alleged in Counts 1, 2, 3, or 4 this indictment, pursuant to Title 18, United States Code, Section 1467, the defendant,

STEVEN ANDEREGG,

shall forfeit to the United States all of his right, title, and interest in:

(1) any obscene material produced, transported, mailed, shipped, or received in the respective offense;

(2) any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from the respective offense; and

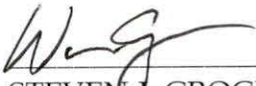
(3) any property, real or personal, used or intended to be used to commit or to promote the commission of the respective offense.

A TRUE BILL



PRESIDING JUROR

Indictment returned: 2024-05-15

 FOR

STEVEN J. GROCKI
Chief, Child Exploitation and Obscenity Section

September 4, 2024

Deepfakes in Legal Proceedings – A Strategic Framework for Collaborative Solutions

Gil Avriel, Jerry Bui, Stephen Dooley, Chris Haley, Ruth Hauswirth, Mary Mack, Dan Regard,

Hon. Judge Xavier Rodriguez, Kaylee Walstad, Paul Weiner

EDRM - Electronic Discovery Reference Model

+ Follow

Contact

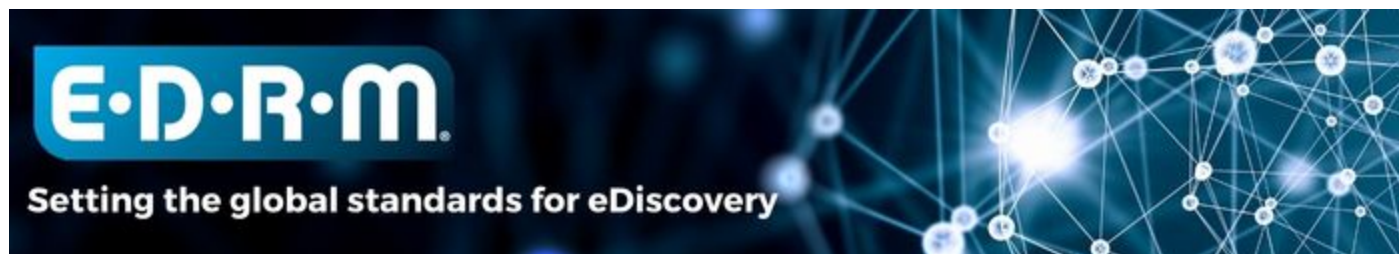


Image: Holley Robinson, EDRM.

What can we do to address the challenge of Deepfakes being presented as relevant and authentic evidence in the justice system?

Deepfake technology poses a **serious challenge** to establishing and rebutting the **authenticity** of **digital exhibits in legal proceedings**. The rapid advancement of **generative AI technology** enables the creation and proliferation of high-quality

Privacy - Terms

community shift the discussion on deepfakes in the justice system from the problem space to a solution-based approach. This effort involves two key steps: first, investigating the EDRM to identify the stages where deepfake legal evidence is likely to be present, and second, highlighting the stakeholders involved at each stage of the EDRM model who can help detect Deepfake Legal Evidence. The findings of this work led to the creation of a new diagram: Deepfake Detection in the eDiscovery Reference Model.

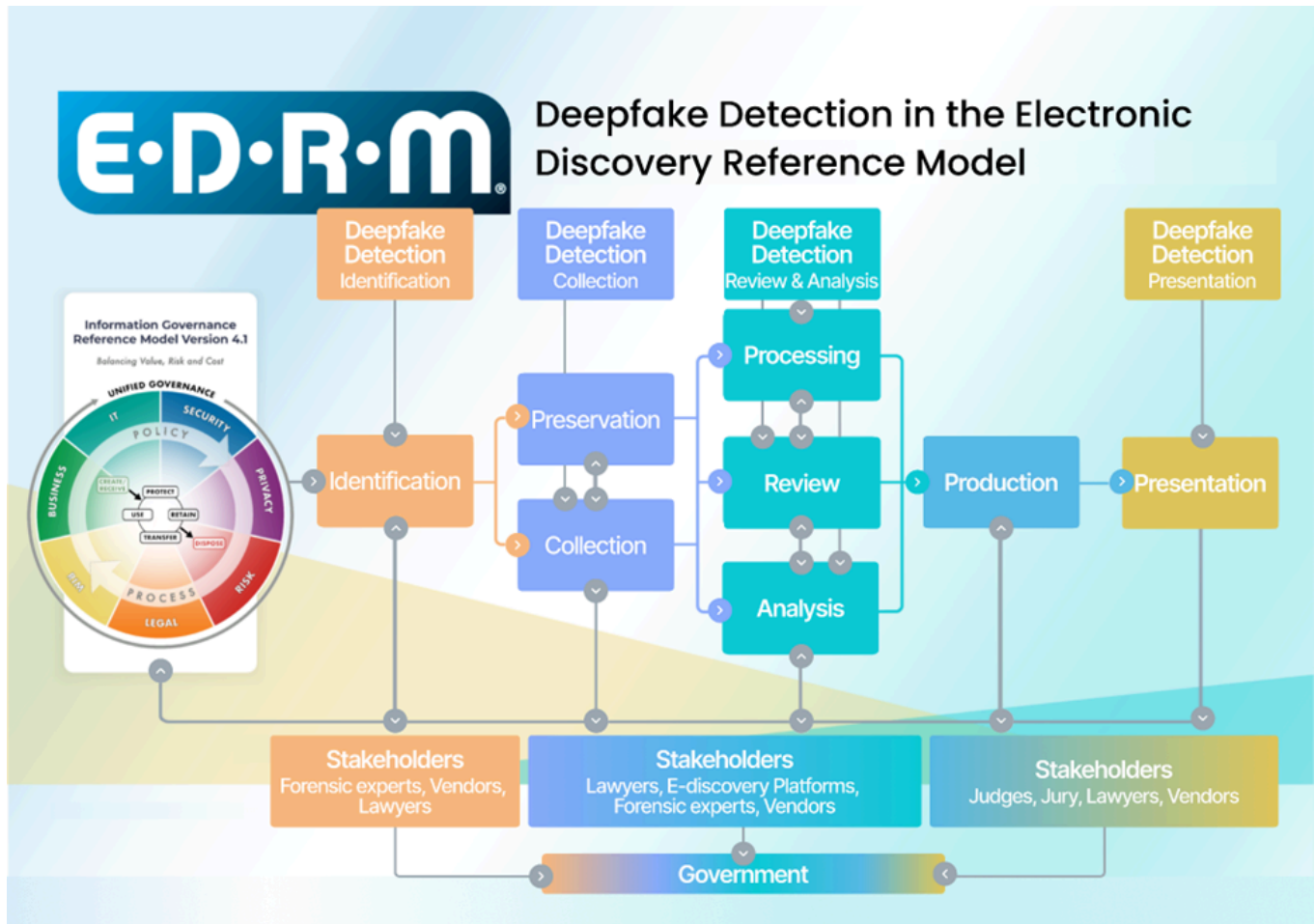


Chart 1

Deepfake Detection in the EDRM, © Creative Commons International 4.0, derived from the original at <https://edrm.net>.

This model helps the eDiscovery community understand three crucial aspects: *where* to look for deepfakes, *who* should look for them, and, when relevant, *where* they can locate themselves on the diagram and collaborate to address this challenge.

Identification and Collection Stages

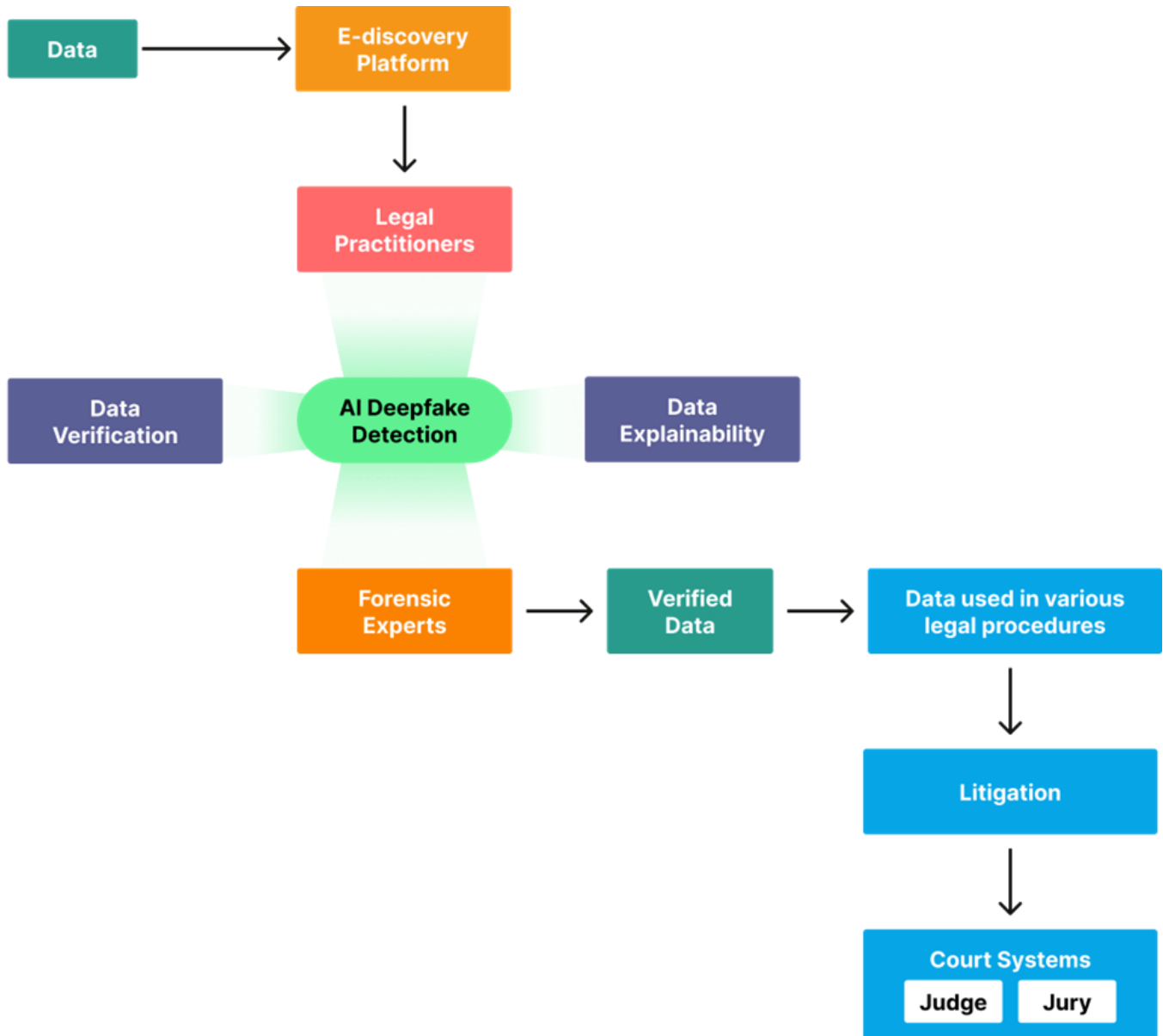


Chart 2

A framework for collaborative solutions.

The Path to Solutions

The new Deepfake Detection in the EDRM is a call for action. Deepfakes in the justice system are becoming a pressing challenge, and we have no time and no choice but to deal with it seriously, responsibly, and systematically. We, the people of law, AI technology, and forensic experts, must collaborate. We have only one justice system, and truth matters. The new Deepfake Detection in the EDRM and the proposed framework for the collaborative technological solution will be presented at the Relativity Fest Annual Conference (Chicago, September 25th-27th) in a panel titled “Deepfakes in eDiscovery: A Joint Framework for Solutions.