ARIZONA SUMMIT ON

ARTIFICIAL INTELLIGENCE

LAW AND THE COURTS

TOPIC: ARTIFICIAL INTELLIGENCE AND DEEPFAKES; PAPER 1

Authored by:

Mark Lanterman

Deepfakes and the Impact of AI on the Courtroom

Mark Lanterman

I. INTRODUCTION

In 2014, Professor Stephen Hawking expressed his weariness over advancements in artificial intelligence, telling the BBC, "The development of full artificial intelligence could spell the end of the human race". Though Hawking himself had a very personal relationship with AI, even making communication possible throughout his battle with ALS, he still feared, "the consequences of creating something that can match or surpass humans."[1] In recent years, AI has only continued to shape how human beings work, learn, and live. The benefits are numerous—from advanced medical technologies to the conveniences afforded by tools such as ChatGPT—and the possibility for new applications seems limitless. The potential is exciting, but equally concerning. Almost ten years later, Stephen Hawking's concerns have resurfaced for many.

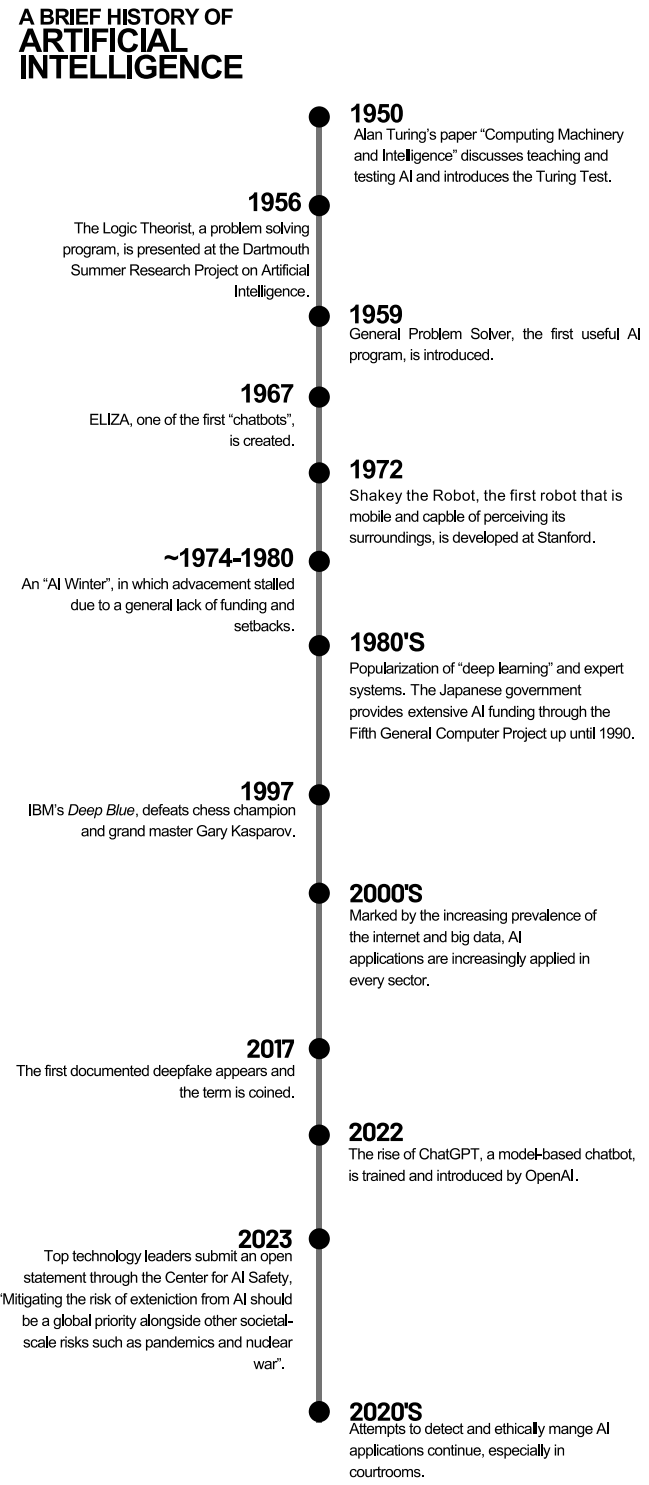
On October 30, 2023, the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence was put forth by the Biden Administration.[2] The executive order acknowledges both the risks and manifold benefits of AI technology, as well as the need for establishing governance in managing these technologies as responsibly as possible. It states:

> *Artificial Intelligence must be safe and secure. Meeting this goal requires robust, reliable, repeatable, and standardized evaluation of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use.… Testing and evaluations, including post-deployment performance monitoring, will help ensure that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed and operated in a secure manner, and are compliant with applicable Federal laws and policies.* ***Finally, my Administration will help develop effective labeling and content provenance mechanisms, so that Americans are able to determine when content is generated using AI and when it is not.***

Courts are being called upon to address AI in multiple forms; from developing standards and policies for using generative AI tools such as ChatGPT in writing court documents to identifying a potential deepfake submitted into evidence. While the executive order of October 2023 puts forth a goal of enabling Americans to be able to immediately "spot" a product of AI, technologies that would allow for this instant identification with complete accuracy are not

[1] https://www.bbc.com/news/technology-30290540

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/



currently available. Though this objective may be achieved at some point in the future, it is important that courts prepare themselves for addressing current issues involving AI. Depending on what technologies are developed and implemented in the future, such as watermarking or labeling systems, it will still be important to have protocols in place for instances in which the veracity of digital evidence remains contested.

In particular, courts need reliable methods to manage deepfake technology, especially as it pertains to detection and in addressing the "deepfake defense". This paper will provide a brief history of advancements in artificial intelligence and deepfake technology, an overview of some of the issues that these technologies present in court, and a proposal for how to best address deepfakes given current technological limitations.

II. BACKGROUND

Well before Stephen Hawking's comments, A.M. Turing's 1950 paper, "Computing Machinery and Intelligence" discussed approaches to teaching and testing machines, though resources and knowledge at that time were not sufficient to begin pursuing AI in earnest. As computing technologies developed, and were less expensive to utilize, so too did advancement in artificial intelligence. Marked by numerous setbacks and the need for computing systems to evolve first, the journey to deepfake technologies and applications such as ChatGPT has been a long one. From

the science fiction fantasies of the early 20th century to today, artificial intelligence has taken up a notable position in modern consciousness. Though once primarily restricted to the academic community, many AI applications are now commonly available.

ChatGPT, a chatbot developed by OpenAI, is one such example. Released in November of 2022, ChatGPT quickly became a popular topic in almost every sector. Once released, ChatGPT was lauded for its potential benefits and uses, but ethical questions about its development and concerns about safety and security soon steered the conversation. OpenAI explains in its blog, "We've trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer followup questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests."[3] From being temporarily banned in Italy to Sam Altman himself, the CEO of OpenAI, admitting to being "a little bit scared of AI",[4] ChatGPT has continued to make international headlines. Within the legal community, problems soon materialized when it came to using ChatGPT in an acceptable way. Many within the legal community are still looking for guidance when it comes to strategically implementing ChatGPT while minimizing the risks. Policies for guiding appropriate use (and when human intervention is necessary to review AI-produced materials) are especially necessary for lawyers tasked with the responsibility of safeguarding their clients' information.

A New York lawyer used ChatGPT to create a legal brief, which was discovered after cited cases were shown to be fabricated.[5] He explained that he had been unaware that ChatGPT could create false information, and expressed remorse for not verifying that the content it produced was accurate. This incident demonstrated the need to create standardized practices for ChatGPT, and AI more generally, when used for legal purposes. It also showed that in spite of ChatGPT's impressive ability to create believable content instantly, human oversight is still needed to ensure its accuracy. Following this incident, U.S. District Judge Brantley Starr of the Northern District of Texas implemented a policy requiring attorneys to "file a certificate to indicate either that no portion of any document they file was generated by an AI tool like ChatGPT, or that a human being has checked any AI-generated text."[6] However, some judges may find this kind of measure to be unwarranted, believing that current standards and ethical responsibilities are sufficient in guiding an attorney's use of AI. In an open letter drafted with the assistance of ChatGPT, Judge Scott U. Schlegel stated his opinion that, "an order specifically prohibiting the use of generative AI or requiring a disclosure of its use is unnecessary, duplicative, and may lead to unintended consequences". Furthermore, he stated that, "Generative AI, much like any tool, is only as effective as the legal expertise guiding it."[7]

In addition to ChatGPT, other types of AI have found their way into the courtroom. While practices are having to be developed to guide how applications such as ChatGPT are used

[3] https://openai.com/blog/chatgpt
[4] https://www.cnbc.com/2023/03/20/openai-ceo-sam-altman-says-hes-a-little-bit-scared-of-ai.html
[5] https://www.nytimes.com/2023/06/08/nyregion/lawyer-chatgpt-sanctions.html
[6] https://www.cbsnews.com/news/texas-judge-bans-chatgpt-court-filing/
[7] https://www.judgeschlegel.com/blog/-a-call-for-education-over-regulation-an-open-letter

within the legal profession, the court is being called upon to recognize instances in which AI is being used by litigants to create fake evidence, or as an excuse to weaken real evidence.

III. THE DEEPFAKE

According to the Department of Homeland Security's paper, "Increasing Threat of Deepfake Identities", "Deepfakes, an emergent type of threat falling under the greater and more pervasive umbrella of synthetic media, utilize a form of artificial intelligence/machine learning (AI/ML) to create believable, realistic videos, pictures, audio, and text of events which never happened. Many applications of synthetic media represent innocent forms of entertainment, but others carry risk."[8] Deepfakes are created using readily available deepfake technology; they are completely manufactured and do not incorporate existing media. Though sometimes made for the purposes of entertainment, they are also frequently used as a method for spreading misinformation.

In addition to deepfakes, shallow fakes can be similarly deceiving. Though the terms are often conflated, shallow fakes use basic editing techniques and software tools to alter existing media, for example by slowing down parts of a video or selective splicing. With one small edit, an entire video can be altered to give a drastically different perspective than its original. This type of modified digital content may be simpler to create than a deepfake, thus making them more common. However, since they are made from an existing source, they may be less challenging to identify. Deepfakes remain difficult to distinguish from authentic content, even for experts. As they are entirely generated using AI technology, several different measures may be needed to make a determination as to whether a piece of evidence is a deepfake.

In one UK case, a shallow fake almost had a critical impact on a child custody case. "A woman said her husband was dangerous and that she had the recording to prove it. Except, it turned out she didn't. The husband's lawyer revealed that the woman, using widely available software and online tutorials, had doctored the audio to make it sound like his client, a Dubai resident, was making threats. . . [and] by studying the metadata on the recording, his experts revealed that the mother had manipulated it."[9] In this instance, a third-party expert was required to analyze the evidence in question and provide insight into its origin. Though the evidence in this situation was shown to be a shallow fake, it is likely that harder-to-identify deepfakes will only continue to proliferate and complicate proceedings.

Still, at the time of writing, many believe that the risk of deepfakes being submitted into evidence is a less pressing threat than that of its reversal—the deepfake defense. Capitalizing on the uncertainty and mistrust characterizing the "misinformation age", a new tactic has arisen among litigants when presented with strong evidence. "That's not me; it's fake. Prove it's not." Though it may seem a weak defense at face value, it can deplete resources, fatigue juries,

[8] https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf
[9] https://www.abajournal.com/web/article/courts-and-lawyers-struggle-with-growing-prevalence-of-deepfakes

and generally prevent a case from moving forward. Depending on the circumstances, it may be difficult to make up for lost time and restore confidence in the evidence as presented.

As both situations continue to play out in the courtroom, courts should be well-equipped to address them. Though judges may not necessarily be directly responsible for identifying deepfakes or altered media, it is important that judges use available measures to gather contextual information and uphold admissibility standards for digital evidence in making authenticity determinations.

IV. THE PROBLEM

Deepfakes are easily generated, easily shared, and can easily fool even the most trained eye. The term deepfake was coined in 2017 after the appearance of what is commonly accepted as the first deepfake; since then, they have become a hallmark of current trends in AI. It should be noted that the best and most convincing deepfakes may require more advanced equipment, processing abilities, and training; however, producing a deepfake is now easier than ever as new tools are introduced to the market. Voice deepfakes (or vocal cloning) can also be eerily convincing. Using AI technology, individuals' voices can be replicated and used to make new recordings.

Deepfakes can pose a two-fold problem in the courtroom. Either deepfakes are admitted as evidence having been maliciously produced by litigants or the deepfake defense will be thrown out indiscriminately to weaken legitimate evidence.

Some believe that the deepfake defense was made in a case involving Tesla and a wrongful death lawsuit.[10] In 2018, Walter Huang died in a car accident while driving a Tesla vehicle. According to the complaint, the vehicle's Autopilot feature did not function properly, leading to Mr. Huang's fatal car accident. His family contends that Tesla misrepresented the risks of the Autopilot feature technology; a statement made by one of the family's attorneys even states that Tesla is guilty of "beta testing its Autopilot software on live drivers."[11]

Huang's family points to a 2016 video of Elon Musk as proof that Tesla and Elon Musk himself have historically overstated the safety of their vehicles. In one video, Elon Musk can be seen stating during a technology conference, "A Model S and Model X at this point can drive autonomously with greater safety than a person. Right now."[12] In response, Musk's legal team stated that not only does Mr. Musk not remember making that specific claim, but that the video itself could be fake. Simply, given Mr. Musk's fame and notoriety, it is possible that the video may be a deepfake.

---

[10] Sz Hua Huang et al v. Tesla, Inc., The State of California, no. 19CV346663

[11] https://www.forbes.com/sites/alanohnsman/2019/05/01/tesla-sued-by-family-of-silicon-valley-driver-killed-in-model-x-autopilot-crash/?sh=63f0dbfe1c3f

[12] https://www.npr.org/2023/05/08/1174132413/people-are-trying-to-claim-real-videos-are-deepfakes-the-courts-are-not-amused

V. STRATEGIES FOR MANAGING DEEPFAKES

Judge Evette Pennypacker responded, "Their position is that because Mr. Musk is famous and might be more of a target for deep fakes, his public statements are immune".[13] Furthermore, "In other words, Mr. Musk, and others in his position, can simply say whatever they like in the public domain, then hide behind the potential for their recorded statements being a deep fake to avoid taking ownership of what they did actually say and do".[14] In light of this claim, the court had to decide how to proceed:

Confronted with Tesla's refusal to rule out that some clips could be digitally altered deep fakes and therefore not suitable as evidence, the judge came up with an elegant solution: Put the billionaire entrepreneur and artificial intelligence enthusiast under oath and have him testify as to which statements coming out of his mouth are authentic.[15]

To gather contextual information, Judge Pennypacker allowed for an apex deposition[16] of Mr. Musk in order to establish whether or not he had a) attended the functions as portrayed in the footage and b) made the statements in question. This measure was ultimately deemed necessary to determine the authenticity of the recording, likely an unintended consequence of the defense.

On this occasion, the deepfake defense resulted in a need for additional testimony to assist in establishing the veracity of digital evidence presented. Following the court's response, one lawyer representing Tesla stated that the intention was not to claim any videos were deepfakes, but "we raised this idea, this issue, because we're living in a world today where these things exist"[17]. And this is, more or less, the unfortunate heart of the issue. Namely, that the emergence of the deepfake has opened the door to the claim that any piece of evidence, could, in theory, be fake. This court's response illustrates the fact that when dealing with new technologies, the old rules can still apply. Gathering contextual information using available means (i.e. apex depositions) and going to the source are critical steps in minimizing any negative ramifications of the deepfake defense.

When it comes to determining the role and responsibilities of the court in verifying digital evidence, some stress that a judge is only responsible for following the rules of evidence. Judges are not expected to be experts in every issue that may appear before them, which has also been true in matters involving digital evidence. However, as is always the case, judges are called upon to make credibility determinations based on testimony and the facts of a case.

---

[13] https://www.reuters.com/legal/elon-or-deepfake-musk-must-face-questions-autopilot-statements-2023-04-26/
[14] https://news.bloomberglaw.com/esg/musk-likely-must-give-deposition-in-fatal-autopilot-crash-suit
[15] https://fortune.com/2023/04/27/elon-musk-lawyers-argue-recordings-of-him-touting-tesla-autopilot-safety-could-be-deepfakes/
[16] https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-seeing-is-not-believing-authenticating-deepfakes
[17] https://fortune.com/2023/04/27/elon-musk-lawyers-argue-recordings-of-him-touting-tesla-autopilot-safety-could-be-deepfakes/

In Rebecca A. Delfino's paper, "Deepfakes on Trial: A Call to Expand the Trial Judge's Gatekeeping Role to Protect Legal Proceedings from Technological Fakery", she submits, "[This article] is the first to propose a new addition to the Federal Rules of Evidence reflecting a novel reallocation of fact-determining responsibilities from the jury to the judge, treating the question of deepfake authenticity as one for the court to decide as an expanded gatekeeping function under the Rules. The challenges of deepfakes—problems of proof, the "deepfake defense," and juror skepticism—can be best addressed by amending the Rules for authenticating digital audiovisual evidence, instructing the jury on its use of that evidence, and limiting counsel's efforts to exploit the existence of deepfakes".[18]

Basic guidelines can help in gathering necessary contextual information.

1. The best defense is proactively upholding authentication standards and the rules of evidence, especially when handling digital media. These measures will best allow for the preservation of original source material, which can be analyzed by third experts should the need arise. When a claim of fake evidence is made, judges can look to how well digital evidence has been managed by both sides as one metric for assessing the likelihood of whether a claim is being made in good faith.

2. Context is key. Additional witness testimony may be required to investigate deepfake claims. Asking specific questions about the evidence at hand, as well as ascertaining how that evidence has been collected, can shape the court's next steps.

3. Third-party forensic experts can be valuable in providing information about a piece of evidence, indicating a probability of its authenticity. A special master appointed by the court can investigate how digital evidence has been handled throughout a case and determine whether best practices have been upheld in the collection, preservation, and analysis of digital evidence. An expert may be able to provide a digital narrative of the evidence in question which may include analyzing original source materials and reporting on any signs of tampering, alteration, or corroborating findings that support claims of inauthenticity. However, it should be noted that is not currently possible to instantly identify a deepfake, or any type of "fake" digital evidence. Can an expert definitively state whether something has been "faked"? Not necessarily. Deepfakes are especially problematic as even technological experts may have difficulty in spotting them. In spite of these challenges, an expert's assessment may be able to supply the court with an additional viewpoint to help inform its own assessment.
4. Expert analysis of digital evidence as well as the gathering of contextual information through deposition and cross-examination can enable the court in its determination (and the assigning of sanctions, if necessary).

[18] https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=4012&context=hastings_law_journal

While costs are a concern when considering utilizing an expert witness, this measure may minimize long term costs incurred due to false claims or the submittal of fake evidence. The burden of the expense can be assigned at the discretion of the judge, perhaps depending on the results of the expert's opinion. Another benefit is that the potential expense may, in fact, deter individuals from making false claims or submitting fake evidence.
Tools designed to detect deepfake technology, though currently at varying degrees of progress and usability, will likely mirror AI in their evolution and development. According to an October 2023 MIT Technology Review article written in response to the goals stated in the Executive Order on AI, "The trouble is that technologies such as watermarks are still very much works in progress. There currently are no fully reliable ways to label text or investigate whether a piece of content was machine generated. AI detection tools are still easy to fool".[19] Part of the evolution of AI is its pursuit of evading detection. At this stage, courts should likely primarily rely on the existing frameworks and systems in place, combined with additional measures to establish context as required.

VI. IN CONCLUSION

Fake evidence is nothing new—but juries existing within a world of "fake news" and readily available, AI technology, is. Courts have to be enabled to manage the new challenges brought about by AI, in the various forms it may appear; from establishing protocols for how materials produced by ChatGPT must be reviewed by counsel, to creating a course of action to manage instances of the deepfake defense. The bad news is that deep fake technology creates undeniable hurdles; the good news is that many of the same protections that existed before for similar issues still apply. And, when in doubt, every tool available should be used to establish context. This may include involving an objective, third party to provide a reliable digital narrative. Though a number of different information-gathering measures may be needed, movement towards improved detection technologies will continue to shape how courts can most efficiently respond.

The legal community should be mindful of the possibility of altered or fake evidence being presented by their clients. Lawyers are never permitted to present evidence that they know for a fact to be false; however, evolving technologies may render more stringent standards necessary.

Ten years ago, Stephen Hawking had clear reservations about the trajectory of artificial intelligence. Nine years later, a statement titled, "Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war", was signed by hundreds of AI, security, and technology leaders.[20] For some, the risk seems overstated. For others, the warning feels appropriate given current problems. Quietly

[19] https://www.technologyreview.com/2023/10/30/1082678/three-things-to-know-about-the-white-houses-executive-order-on-ai/
[20] https://www.safe.ai/statement-on-ai-risk

progressing, 2023 seemed to be the year when many began to share a common sentiment with Hawking and others throughout the years who have expressed their concerns.

Even OpenAI founder, Sam Altman, urged increased regulation and oversight at a Senate subcommittee hearing in May of 2023.[21] As the October 2023 Executive Order explains:

> *Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.*

Society is undoubtedly having to grapple with balancing the numerous benefits of these technologies with their significant risks. In the courtroom, existing evidentiary rules can form the basis of how deepfakes, and the deepfake defense, are addressed. Calling for additional testimony, and the input of expert witnesses, are measures that can allow the court to gather contextual information in determining the admissibility of evidence.

[21] https://www.nytimes.com/2023/05/16/technology/openai-altman-artificial-intelligence-regulation.html

MINNESOTA STATE BAR ASSOCIATION

OCTOBER 2023

BENCH+BAR of Minnesota

READING THE FINE PRINT

The extensive changes to Minnesota landlord-tenant law

Deepfakes, AI, and digital evidence

BY MARK LANTERMAN ✉ *mlanterman@compforensics.com*

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

With the ever-expanding prevalence of artificial intelligence, I'm sure that most of us have seen at least a few types of "deepfakes." Elvis Presley singing the latest top hits. Albert Einstein answering viewers' questions about life. Living portraits of old photographs. Or some more problematic examples, such as a menacing speech by Mark Zuckerberg or a video of a politician created to spread disinformation. Some may have even seen a video appearing to depict their company's CEO requesting an immediate wire transfer, as cybercriminals continue to use AI to bolster social engineering campaigns. It seems that just about everybody now has the ability to alter digital media, with varying degrees of believability.

Deepfakes, or digitally altered media that convincingly make one individual appear as another, have also had an impact on the courtroom. According to the Department of Homeland Security's paper, "Increasing Threat of Deepfake Identities," "Deepfakes... utilize a form of artificial intelligence/machine learning (AI/ML) to create believable, realistic videos, pictures, audio, and text of events which never happened. Many applications of synthetic media represent innocent forms of entertainment, but others carry risk."[1] While there have been cases of litigants attempting to enter a deepfake into evidence, the problem has also been reversed–litigants claiming that real evidence has been manipulated or fabricated.

Digitally stored information has repeatedly proved itself to be a pivotal source of evidence, often serving as a critical, unbiased witness. Nearly every case today involves ESI to some extent. When presented with this kind of strong, perhaps damning, evidence, people now have the ability to throw a new defense at the wall and see if it sticks: "It's not real." While a judge may reject the attempt,[2] the "deepfake defense" will still have consequences. As an NPR report about the phenomenon noted, "If accusations that evidence is deepfaked become more common, juries may come to expect even more proof that evidence is real."[3] Though the technology is relatively new, courts already have processes in place to handle fake evidence and can apply these same procedures to managing deepfakes.[4] But courts are less prepared to deal with proving that real evidence is, in fact, real. Furthermore, the better the evidence, the more likely that juries will feel required to verify its legitimacy. With the rise of common applications of artificial intelligence, the pressure is on to verify digital evidence as efficiently as possible.

Deepfakes present a host of legal concerns. From actors losing the rights to their own identities to reputational damage to manufactured evidence affecting the outcomes of custody disputes, we are just beginning to learn how to grapple with deepfakes and artificial intelligence. In the courtroom, well-communicated guidelines, strong authentication standards, and extensive training can address some of the risks. Expectations for juries surrounding the requirements for evidence verification should be well-established, and court-appointed digital forensic experts can manage and analyze digital evidence for both sides, helping to create an even playing field and manage costs.

Emerging laws and regulations will hopefully begin to help the legal community navigate new problems posed by these technologies. But developing tried-and-true methods to identify deepfakes reliably will undoubtedly remain a work in progress. Given how difficult it can be to spot a deepfake, the New York Times wrote recently, "Initiatives from companies such as Microsoft and Adobe now try to authenticate media and train moderation technology to recognize the inconsistencies that mark synthetic content. But they are in a constant struggle to outpace deepfake creators who often discover new ways to fix defects, remove watermarks and alter metadata to cover their tracks."[5]

In the meantime, members of the legal community should be on high alert for the possibility of altered digital media, from opposing parties and their own clients. Attorneys should strive to be especially vigilant in abiding by digital-evidence best practices throughout the entirety of a case. In the event that third-party verification is ultimately required, organizing original source material and making it readily available is essential. ▲

NOTES

1 *https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf*

2 *https://www.npr.org/2023/05/08/1174132413/people-are-trying-to-claim-real-videos-are-deepfakes-the-courts-are-not-amused*

3 *Id.*

4 *Id.*

5 *https://www.nytimes.com/2023/01/22/business/media/deepfake-regulation-difficulty.html*

MINNESOTA STATE BAR ASSOCIATION

DECEMBER 2023

BENCH+BAR of Minnesota

LEGAL TECH TRENDS

TRANSFORMING THE PRACTICE OF LAW

Biden issues ambitious executive order on AI

BY MARK LANTERMAN ✉ *mlanterman@compforensics.com*

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

On October 30, the Biden administration issued its Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[1] Coming near the end of what was dubbed by many "the year of AI," the order acknowledges both the risks and manifold benefits of AI technology, as well as the need for governance oversight to manage it as responsibly as possible. The order states:

> "Artificial Intelligence must be safe and secure. Meeting this goal requires robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use...Testing and evaluations, including post-deployment performance monitoring, will help ensure that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed and operated in a secure manner, and are compliant with applicable Federal laws and policies. Finally, my Administration will help develop effective labeling and content provenance mechanisms, so that Americans are able to determine when content is generated using AI and when it is not."

In the "misinformation" age, marked by deep fakes, vocal cloning, and the unsettling idea that seeing shouldn't always be believing, a labeling system allowing Americans to spot AI-generated content would certainly be a game-changer. Within a year, it is expected that the government will have a better idea of how to best identify and label "synthetic content produced by AI systems, and to establish the authenticity and provenance of digital content, both synthetic and not synthetic, produced by the Federal Government or on its behalf." While these efforts seem to be primarily directed at digital content produced by the United States government, it is less clear how such measures would be applied to AI-produced content more generally.

The idea of an identification system itself is promising in light of current challenges, and the executive order signals progress in the right direction, but it remains to be seen how these objectives will come to fruition. For example, the order describes watermarking as "the act of embedding information, which is typically difficult to remove, into outputs created by AI." However, as noted by MIT Technology Review, "The trouble is that technologies such as watermarks are still very much works in progress. There currently are no fully reliable ways to label text or investigate whether a piece of content was machine generated. AI detection tools are still easy to fool. The executive order also falls shorts of requiring industry players or government agencies to use these technologies."[2] At this point in time, enabling Americans to distinguish AI-generated content from authentic content will still require a substantial amount of time and effort on several different fronts.

Furthermore, the order's call for AI applications to be made resilient against misuse or dangerous modifications will be similarly difficult. As is common with rapidly evolving technology, the methods needed to use or adapt it for nefarious purposes tend to develop at the same rate. Though the objectives of the order are welcome, and likely reflect the wishes of the American people when it comes to navigating a world infiltrated by "fake news," they will be challenging to achieve. In the meantime, especially in the courtroom, policies and procedures should be considered for the here and now. From the deepfake defense ("That's not me, prove it is") to fake content being submitted as evidence, methodologies should be established for managing AI in the courtroom in the absence of widescale, standard technological detection methods.

The executive order indicates that AI's inherently dual-sided nature is being acknowledged within government. However, legislation is still required to effectively combat its risks and maximize benefits. Some of the proposed objectives are still elusive, and it is unclear when individuals can be expected to consistently spot a deepfake in daily life or at the very least be assured that the government communications they receive are real. That being said, improved governance, safety protocols, transparency, and a commitment to testing are all positive goals that would assist in making better protections for consumers a reality. ▲

NOTES

[1] *https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/*

[2] *https://www.technologyreview.com/2023/10/30/1082678/three-things-to-know-about-the-white-houses-executive-order-on-ai/*

MINNESOTA STATE BAR ASSOCIATION

MAY/JUNE 2023

BENCH+BAR of Minnesota

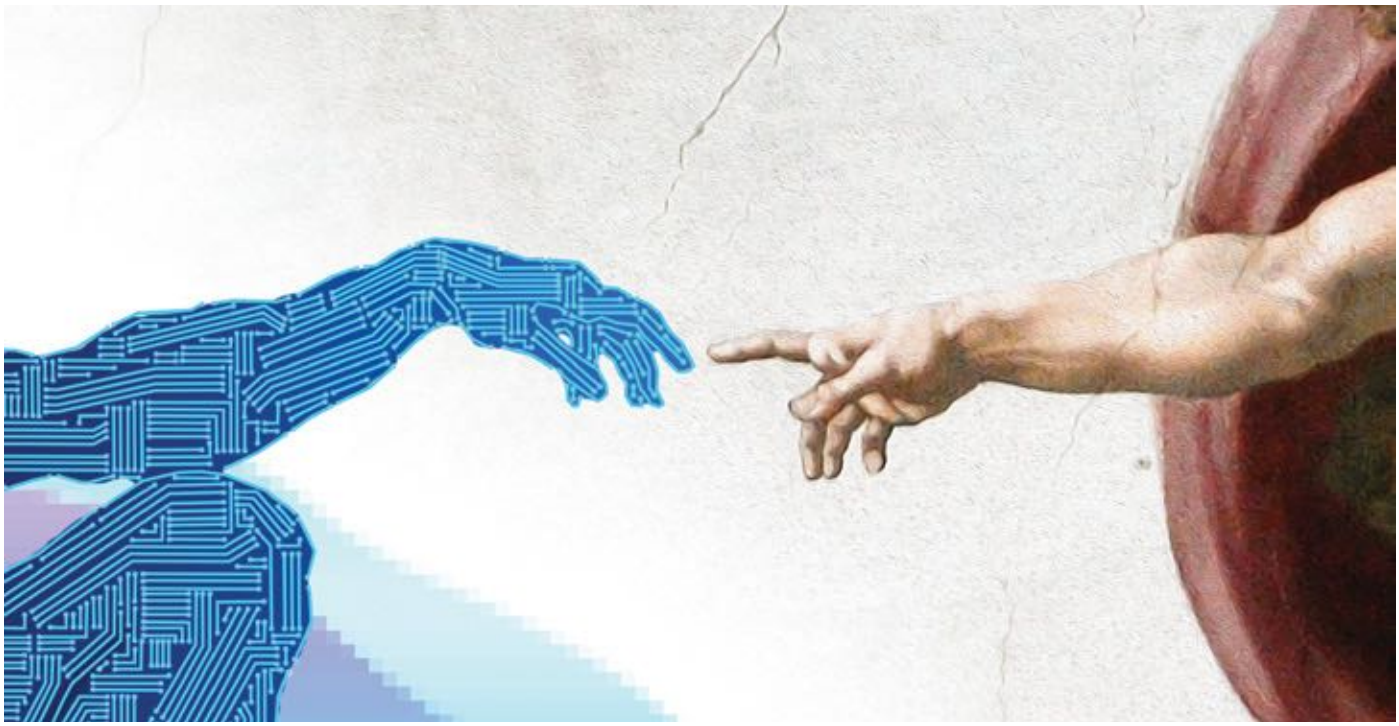
We need to talk about ChatGPT

A lawyer's introduction to the exploding field of AI and large language models

THIS ARTICLE IS HUMAN-WRITTEN

ChatGPT and navigating AI

BY MARK LANTERMAN ✉ *mlanterman@compforensics.com*



MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

Since its release in November 2022, ChatGPT has been met with a wide variety of responses. It's been praised for passing the bar exam.[1] It's been feared for its potential to replace certain jobs. It's been banned in Italy (at least temporarily). Its inherent security and privacy risks have been acknowledged, along with its potential for improving cybersecurity postures. AI has been a much-discussed topic in recent months, and with good reason.

In an open letter titled "Pause Giant AI Experiments" from the Future of Life Institute, signed by the likes of Elon Musk and Steve Wozniak, the question is posed: "*Should* we develop nonhuman minds that might eventually outnumber, outsmart, obsolete and replace us?... Powerful AI systems should be developed only once we are confident that their effects will be positive and their risks will be manageable."[2] The letter asks for a six-month pause on training for "AI systems more powerful than GPT-4," and calls for increased governance, safety protocols, and improvements in accuracy and transparency. The letter was recently referenced by a group of European Union members requesting a global summit on AI to establish governance for its "development, control, and deployment." In an open letter from these EU lawmakers, responsibility and internal cooperation are highlighted as necessary components in ensuring that progress in AI remains "human-centric, safe, and trustworthy."[3]

The utilization of new technology always comes with a caveat—namely, that gains in convenience result in losses to security. AI, and the ubiquity of ChatGPT more specifically, have presented an especially complex and multifaceted conundrum for individuals, organizations, firms, governments, and security professionals, to name a few. The potential benefits seem overwhelming—reduced time spent on simple tasks, improved efficiency in problem-solving, and limited costs to clients being prime examples. In the words of a recent ABA Journal column, "Despite its current shortcomings, ChatGPT has the potential to significantly enhance efficiency in the delivery of legal services... It can be a tremendous time-saver and is a great place to start your research on just about any topic. But whether you use ChatGPT for personal or professional reasons, you'll need to have a full understanding of the issue at hand and should thoroughly review, edit and supplement any results or draft language it provides you."[4]

First drafts, letters, and correspondence with clients could all be supported with the use of AI.

But actually using the information generated by AI tools requires a great deal of discretion and careful review. As of right now, inaccuracies, false information, and misleading statements abound. The time required to fact check, and the efforts required to mitigate any problems resulting from an error slipping through the cracks, may diminish or even negate the convenience factor. Furthermore, many observers are acknowledging the possible negative impact on new lawyers, with AI taking away opportunities for valuable experience. This reality is of great concern outside the legal community as well, as AI may begin to replace the skillsets of human beings. Additionally, ethical questions have arisen as to what can be legally used from a chatbot conversation, since it may contain trademarked, copyrighted, or simply false information.[5]

The double-edged nature of AI is similarly challenging from a cybersecurity perspective. The benefits may include an improved ability to automate security measures, including those needed for monitoring and detection.[6] But it can also be utilized by cybercriminals to assist in the creation of malware or more convincing phishing attacks. Notably, ChatGPT suffered its own data breach in March, which resulted in the leak of users' personal information and conversation content.[7]

The all-too-critical human element of security especially comes into play when analyzing the risks and benefits of this tool. When any new technology is incorporated into an organization, it is important to fully map out how that technology will be used, and then communicate that information clearly to employees. While ChatGPT urges users to avoid entering sensitive information into conversations,[8] confidential data and personal identifiable information are being entered nonetheless; in some instances, employees themselves are entering confidential company information, constituting a data breach. The tool itself is trained on vast amounts of data gathered from the internet, further blurring an important question—is it ethical to use ChatGPT, given the way it was, and continues to be, trained? If yes, what parameters should be created to regulate its use? If no, how will future AI projects be regulated?

At the time of this writing, Italy has banned ChatGPT, citing violations against the European General Data Protection Regulation (GDPR): "OpenAI doesn't have age controls to stop people under the age of 13 from using the text generation system; it can provide information about people that isn't accurate; and people haven't been told their data was collected. Perhaps most importantly, its fourth argument claims there is 'no legal basis' for collecting people's personal information in the massive swells of data used to train ChatGPT."[9] In spite of this list, it may be reinstated by the time you read this should OpenAI comply with a set of hard and fast rules required by the Italian Data Protection Authority. Regardless of the outcome, overarching concerns surely remain.

For a lot of us, the recent conversations surrounding chatbots and AI may feel like a sci-fi movie, with robots overpowering humans and taking over the world. What happens when technology gets *too* smart, if the conveniences afforded by technology become *too* convenient, literally replacing the very human beings who created it and allowed it to flourish? It's certainly an interesting (if scary!) thought, and while not everyone concurs with such an alarming viewpoint, the rapid development of AI certainly requires political attention, careful planning in its applications, and a complete-as-possible assessment of its extensive societal impact.

For the legal community, the question of how to best implement AI will likely be complicated as these issues unfold. While it seems safe to say that many, if not most, organizations will soon be using AI at least in some capacity, law firms are always held to a higher standard in managing client data and ensuring a strong security posture. Though the immediate benefits of a quickly written draft or assistance in correspondence may be tempting, be sure to bide your time in approaching AI and establishing how it will be incorporated into your firm. Specify what data can be entered into conversations, train employees in appropriate use, and establish guidelines for how your firm will use the tool in the most productive and secure way possible. ▲

NOTES

[1] *https://www.abajournal.com/web/article/latest-version-of-chatgpt-aces-the-bar-exam-with-score-in-90th-percentile*

[2] *https://futureoflife.org/open-letter/pause-giant-ai-experiments/*

[3] *https://www.cnbc.com/2023/04/17/eu-lawmakers-call-for-rules-for-general-purpose-ai-tools-like-chatgpt.html*

[4] *https://www.abajournal.com/columns/article/the-case-for-chatgpt-why-lawyers-should-embrace-ai*

[5] *https://news.bloomberglaw.com/us-law-week/employers-should-consider-these-risks-when-employees-use-chatgpt*

[6] *https://www.forbes.com/sites/forbestechcouncil/2023/03/15/how-ai-is-disrupting-and-transforming-the-cybersecurity-landscape/?sh=2c41fff34683*

[7] *https://openai.com/blog/march-20-chatgpt-outage*

[8] *https://help.openai.com/en/articles/6783457-what-is-chatgpt*

[9] *https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/*

MINNESOTA STATE BAR ASSOCIATION

JULY 2023

BENCH + BAR of Minnesota

MSBA PRESIDENT 2023-24

PAUL FLOYD

The artful lawyer

ChatGPT: *The human element*

BY MARK LANTERMAN ✉ *mlanterman@compforensics.com*

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

ChatGPT is continuing to make headlines. It seems like the talk surrounding AI is continuing to evolve as well. Sam Altman, the CEO of OpenAI, admits that even he is a little afraid of the possibilities.[1] On May 16, Altman told a Senate Judiciary subcommittee that "regulatory intervention by governments will be critical to mitigate the risks of increasingly powerful models."[2] During this hearing, Altman highlighted the double-edged nature of AI—the potential loss of jobs, but likewise the potential creation of new jobs; the risk of voter fraud and misinformation, but also the ways in which AI can be used to counter these issues.

The May 16 hearing is being seen by many commentators as what one called "the beginning of what will likely be a long, but broadly bipartisan, process regulating the use of AI and its amazing promise.... [A] regulatory roadmap is beginning to coalesce."[3] Altman proposed strict adherence to safety requirements and extensive testing processes in AI development, all within the structure of federal regulation and oversight. Acknowledging the great potential for worldwide harm as a result of misused or unrestrained AI technologies, Altman emphasized the need for government and industry collaboration and transparency.

Last month I wrote that ChatGPT was still banned in Italy owing to numerous privacy concerns ("This article is human-written: ChatGPT and navigating AI," May/June Bench & Bar). Since then, it's been reinstated after adding certain disclosures and controls.[4] This episode illustrates the tweaks to AI's functioning that will likely continue to be made. In the meantime, however, some of the previously hypothetical crises have indeed come to fruition.

In May, a New York City attorney was found to have used ChatGPT to find case citations for court documents.[5] When these citations were found to be fake, he admitted to using ChatGPT in conducting his research. In a sworn affidavit, he stated that he has "never utilized Chat GPT as a source for conducting legal research prior to this occurrence and therefore was unaware of the possibility that its content could be false."[6] As with any new technology that an organization may plan on incorporating, it is critical to conduct research and create a plan for how it will be best implemented. A quick Google search easily reveals that ChatGPT is rather notorious for giving misleading or even completely false information in conversations. In this case, the consequences for not knowing ChatGPT's weaknesses have been steep.

Partly in response to this event, restrictions are being adopted to manage AI in the courtroom. U.S. District Judge Brantley Starr of the Northern District of Texas, for example, "has ordered attorneys to attest that they will not use ChatGPT or other generative artificial intelligence technology to write legal briefs because the AI tool can invent facts."[7] Though Judge Starr acknowledged some possible uses of the technology that could be appropriate in other situations, he banned using AI alone for legal briefing given its unreliability. Regardless of its application, verifying the authenticity and accuracy of what ChatGPT produces is the user's responsibility, especially within the legal community.

In addition to the ethical issues on display in this particular case, ChatGPT is even being viewed by some as a harbinger of the end—human extinction. What will happen when jobs are replaced by AI? What if life as we know it is taken over by "minds" more powerful than ours? This alarmist view is tempered by the idea that this is a tool that can be used carefully and efficiently to improve human life, not tear it asunder.

Within the cybersecurity field, many experts believe that AI holds the key in combatting the ever-growing number and variety of cyberattacks that are perpetrated daily. If AI can be used to develop sophisticated phishing campaigns, maybe AI is the best resource we have to combat those types of attacks. As far as detection and mitigation goes, ever-evolving AI could be a deal breaker in how organizations scan and respond to cyberattacks. But some take it even a step further. Could AI possibly be the foolproof cybersecurity solution we've been hoping for all along?

Maybe not. In his recently published book, *Fancy Bear Goes Phishing: The Dark History of the Information Age in Five Extraordinary Hacks,*[8] Yale Professor Scott J. Shapiro describes the dangers of solutionism, especially within the realm of cybersecurity. He explains that cybersecurity technology tools are often touted as the best of the best, with AI frequently being the deciding factor as to what makes one product better than any other. But Shapiro goes on to point out that technological fixes are not always what's needed to correct cybersecurity problems. "Cybersecurity is not a primarily technological problem that requires a

primarily engineering solution," he writes. "It is a human problem that requires an understanding of human behavior." Similarly, though ChatGPT "passed" the bar,[9] it is not bound to the same standards required of an actual attorney, who must be qualified to deal with "human problems." Judge Starr further highlights this disqualifying feature of AI in his ban: "Unbound by any sense of duty, honor, or justice, such programs act according to computer code rather than conviction, based on programming rather than principle."[10]

Though I frequently discuss the "human element" of cybersecurity, I think the prevalence of AI and the fears surrounding its ascent are making us all question the "human element" in other industries. For one, AI poses a data security risk—consider an employee who inputs confidential data into a conversation. Or a breach that compromises chat history. But AI may also pose a greater "security" risk as many see it—the risk to human beings' way of life. Within the legal community, it's been challenging to weigh the risks and benefits, as both seem abundant. Ethical guidelines and governance rules will undoubtedly continue to be created to manage the strengths of AI in relation to its pitfalls. In the meantime, it is important to keep an eye on how AI is being used today. Establishing firm requirements for its use and setting clear expectations can help mitigate risk. ▲

NOTES

[1] *https://www.cnbc.com/2023/03/20/openai-ceo-sam-altman-says-hes-a-little-bit-scared-of-ai.html*

[2] *https://www.cnn.com/2023/05/16/tech/sam-altman-openai-congress/index.html*

[3] *https://www.forbes.com/sites/michaelperegrine/2023/05/17/sam-altman-sends-a-message-to-corporate-leaders-on-ai-risk-management/?sh=42ab1e96dbef*

[4] *https://www.bbc.com/news/technology-65431914#*

[5] *https://www.forbes.com/sites/mattnovak/2023/05/27/lawyer-uses-chatgpt-in-federal-court-and-it-goes-horribly-wrong/?sh=4a4c089d3494*

[6] *https://storage.courtlistener.com/recap/gov.uscourts.nysd.575368/gov.uscourts.nysd.575368.32.1_1.pdf*

[7] *https://www.cbsnews.com/news/texas-judge-bans-chatgpt-court-filing/*

[8] Shapiro, Scott. J. *Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks,"* Farrar, Straus and Giroux, 2023.

[9] *https://www.abajournal.com/web/article/latest-version-of-chatgpt-aces-the-bar-exam-with-score-in-90th-percentile*

[10] *https://www.txnd.uscourts.gov/judge/judge-brantley-starr*