



DEVELOPING
AI POLICIES
AND STANDARDS

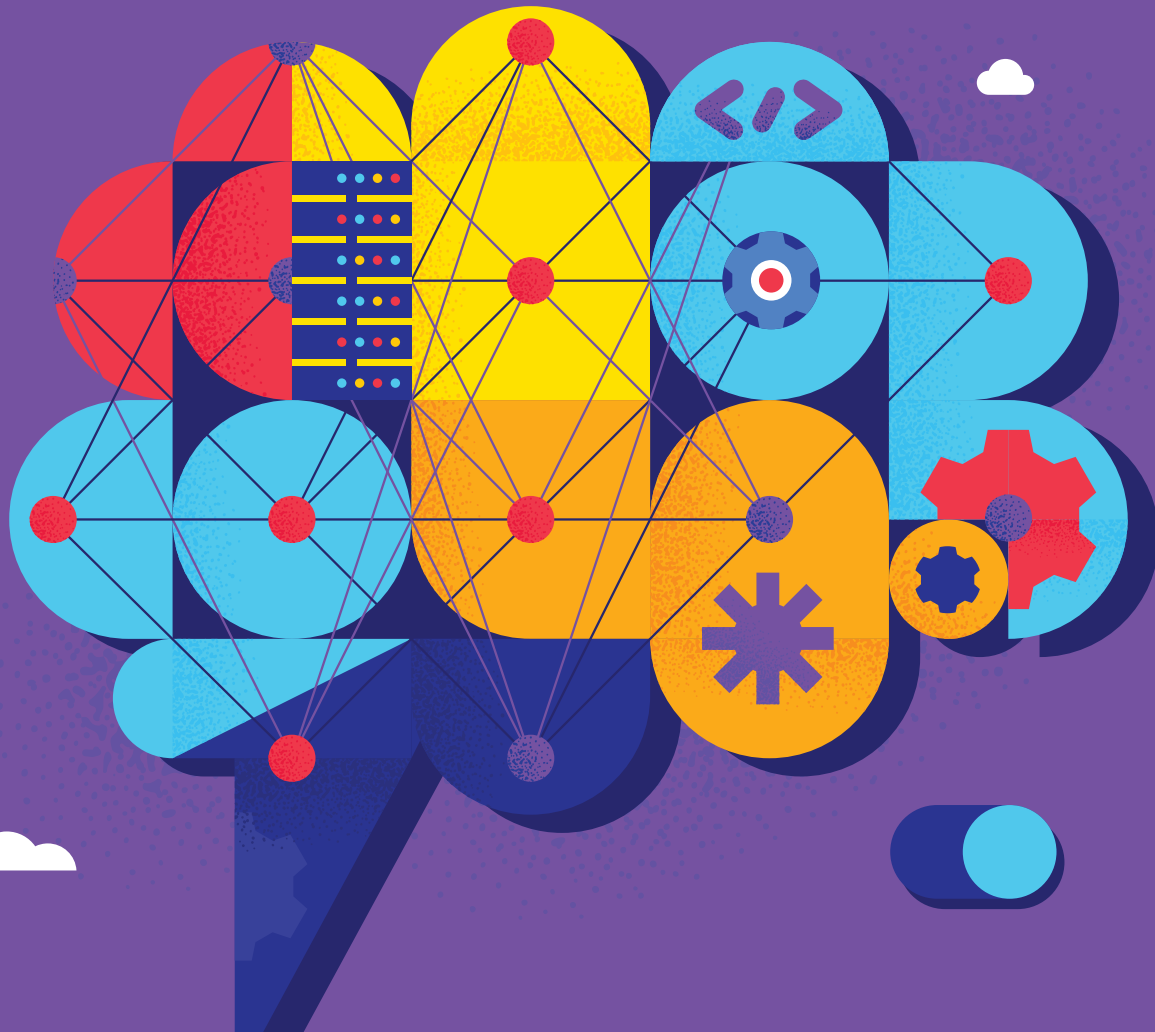
DEEPPAKES AND
MALPRACTICE
RISKS

PRIVACY AND
COPYRIGHT
CONCERNS

VOL 20, NO 3
SPRING 2024

TheSciTechLawyer

A PUBLICATION OF THE AMERICAN BAR ASSOCIATION | SCIENCE & TECHNOLOGY LAW SECTION



ARTIFICIAL INTELLIGENCE

MATTHEW HENSHON
ISSUE EDITOR

Published in The SciTech Lawyer, Volume 20, Number 3, Spring 2024. © 2024 American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

EDITORIAL BOARD

EDITOR-IN-CHIEF

LARRY W. THORPE
Springfield, TN
larrywthorpe@comcast.net

SENIOR EDITORS

MICHAEL A. AISENBERG
Mitre Corp.
McLean, VA
maisenberg@comcast.net

MATTHEW HENSHON
Henshon Klein LLP
Boston, MA
mhenshon@henshon.com

HON. RODERICK KENNEDY
Albuquerque, NM
brazolargo@me.com

PETER F. MCLAUGHLIN
Boston, MA
peterfmclaughlin@outlook.com

LOIS D. MERMELSTEIN
The Law Office of
Lois D. Mermelstein
Austin, TX
lois@loismermelstein.com

CAROL WILLIAMS
Aberystwyth University
Ceredigion, Wales UK
cas55@aber.ac.uk

ASSISTANT EDITORS

PETER J. GILLESPIE
Laner Muchin, Ltd.
Chicago, IL
pgillespie@lanermuchin.com

ROBERT KNAIER
Fitzgerald Knaier LLP
San Diego, CA
rknaier@fitzgeraldknaier.com

LISA R. LIFSHITZ
Torkin Manes LLP
Toronto, ON
llifshitz@torkinmanes.com

SARAH E. MCMILLAN
McGlinchey Stafford PLLC
New Orleans, LA
semcmillan@mcglinchey.com

BRIAN SCARPELLI
ACT | The App Association
Washington, D.C.
bscarpelli@actonline.org

CHRISTOPHER A. SUAREZ
Step toe & Johnson LLP
Washington, D.C.
csuarez@step toe.com

TOMMY TOBIN
Perkins Coie LLP
Seattle, WA
ttobin@perkinscoie.com

**SCIENCE & TECHNOLOGY
LAW SECTION OFFICERS**

CHAIR

LAURA POSSESSKY
Corporation for Public Broad-
casting
Washington, D.C.
lpossessky@cpb.org

CHAIR-ELECT

JOAN R.M. BULLOCK
joan@reformedlawprof.com

VICE CHAIR

LOIS D. MERMELSTEIN
The Law Office of
Lois D. Mermelstein
Austin, TX
lois@loismermelstein.com

SECRETARY

MATTHEW HENSHON
Henshon Klein LLP
Boston, MA
mhenshon@henshon.com

BUDGET OFFICER

CHRISTOPHER A. SUAREZ
Step toe & Johnson LLP
Washington, D.C.
csuarez@step toe.com

SECTION DELEGATES

RICHARD L. FIELD
Cliffside Park, NJ
field@pipeline.com

LUCY THOMSON

Livingston PLLC
Washington, D.C.
lucythomson.aba@mindspring.
com

IMMEDIATE PAST CHAIR

GARTH B. JACOBSON
CT Corporation
Seattle, WA
gbjacobson@hotmail.com

PAST CHAIR LIAISON

TO OFFICERS
HUGH BUTLER WELLONS
Spilman Thomas & Battle PLLC
Roanoke, VA
hwellons@spilmanlaw.com

**AMERICAN BAR
ASSOCIATION
CONTACTS**

DIRECTOR

BARBARA MITCHELL
barbara.mitchell@americanbar.
org

ABA PUBLISHING EDITOR

LORI LYONS
lori.lyons@americanbar.org

ART DIRECTOR

SARA WADFORD
sara.wadford@americanbar.org

ADVERTISING REPRESENTATIVE

CHRIS MARTIN
(410) 584-1905
chris.martin@wearemci.com

SECTION EMAIL ADDRESS

stserve@americanbar.org

MEMBERSHIP QUESTIONS OR ADDRESS CHANGES

1-800-285-2221 or service@americanbar.org

The SciTech Lawyer (ISSN 1550-2090) is published quarterly as a service to its members by the Science & Technology Law Section of the American Bar Association, 321 North Clark Street, Chicago, IL 60654-7598. It endeavors to provide information about current developments in law, science, medicine, and technology that is of professional interest to the members of the ABA Science & Technology Law Section. Any member of the ABA may join the Section by paying its annual dues of \$60. Subscriptions are available to nonmembers for \$75 a year by contacting the ABA Service Center, American Bar Association, 321 North Clark Street, Chicago, IL 60654-7598; 1-800-285-2221. Digital subscription packages for ABA periodicals are available through HeinOnline. If interested, former print subscribers and ABA non-members can visit www.heinonline.org for more information. Requests to reprint articles should be sent to ABA Copyrights & Contracts, www.americanbar.org/reprint; please send all other correspondence to The SciTech Lawyer Managing Editor Lori Lyons, lori.lyons@americanbar.org. For more information, visit ambar.org/SciTechMagazine. The materials contained herein represent the opinions of the authors and editors and should not be construed to be those of either the American Bar Association or The Science & Technology Law Section unless adopted pursuant to the bylaws of the Association. The materials contained herein are not intended as and cannot serve as a substitute for legal advice. Readers are encouraged to obtain advice from their own legal counsel. These materials and any forms and agreements herein are intended for educational and informational purposes only. Copyright © 2024 American Bar Association. All rights reserved.

MESSAGE FROM THE CHAIR

By Laura Possessky

THE IMITATION GAME



Can a machine think? Alan Turing's answer in 1950 was the "imitation game." In a blind test, he posited, if an individual submits a written question to both a person and a computer, and the computer presents a response indiscernible from the human one, then the computer wins the imitation game.

This issue delves into the challenges of a reality where computers can produce responses that are as good as—if not better than—humans. Like humans, computers are not infallible. Bias, hallucinations and other potential problems with computer logic and outcomes present questions about how AI technology should be implemented, managed, and maintained. As lawyers, we must consider the legal and moral frameworks to adopt for responsible use of AI technologies.

Addressing these issues is an ABA priority. This year, ABA President Mary Smith established the ABA's Presidential Task Force on the Law and Artificial Intelligence to ask hard but necessary questions around the development, use, and oversight of AI both within the profession and in society at large. AI impacts on legal research, legal documents, and courtroom evidence will have sweeping implications for rule of law and the administration of justice. We must also evaluate risks and liability that arise when reliance on AI has unintended consequences.

Yet, AI also has promise for legal education and access to justice and could transform the practice of law. Particularly at a time when social media proliferate deepfakes and subversive messaging that undermine democratic processes, scientists and lawyers must ask hard moral questions and press for regulatory frameworks to ensure responsible and transparent use of AI.

SciTech is a part of these discussions. Our annual AI and Robotics National Institute scheduled for October 14–15, 2024, and the work of our Artificial Intelligence and Scientists and the Social Good Committees dedicate deep thought and discussion to these issues.

As we grapple with the novel challenges of AI, we can glean lessons from the wisdom of the past. Scientists who developed the technologies we have today raised deep moral and ethical questions in their time about the application of their discoveries. In a 1940 interview on *I Am An American*, Albert Einstein was asked how scientific discoveries can be turned from our destruction to our advantage. He replied:

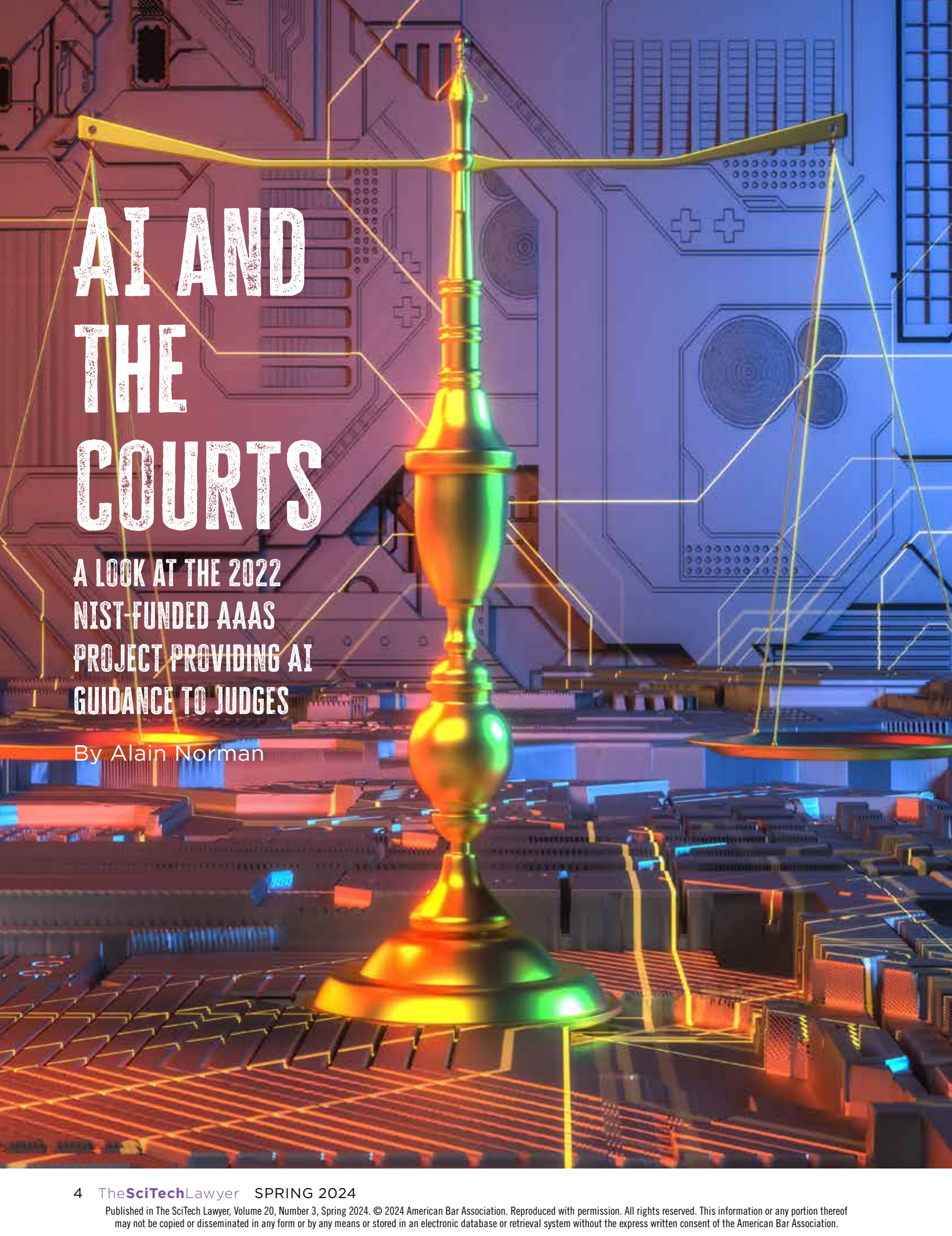
Science has provided the possibility of liberation for human beings from hard labor, but science itself is not a liberator. It creates means not goals. Man should use [Science] for reasonable goals. When the ideals of humanity are war and conquest, those tools become as dangerous as a razor in the hands of a child of three. We must not condemn man's inventiveness and patient conquest of the forces of nature because they are being used wrongly and disobediently now. The fate of humanity is entirely dependent upon its moral development.

Einstein's words resonate today. All of us can offer valuable perspectives on the impact of AI on society and the human condition—as long as we take the time to weigh these deep philosophical questions now.

Please feel free to reach out to me at laura@dcbarista.com with any comments or questions or to find ways to become involved in the SciTech Section.

CONTENTS

- 2 **MESSAGE FROM THE CHAIR**
BY LAURA POSSESSKY
- 4 **AI AND THE COURTS: A LOOK AT THE 2022 NIST-FUNDED AAAS PROJECT PROVIDING AI GUIDANCE TO JUDGES**
BY ALAIN NORMAN
- 8 **NAVIGATING THE PATCHWORK OF AI LAWS, STANDARDS, AND GUIDANCE**
BY EMILY MAXIM LAMM
- 12 **DEEPFAKES AND MALPRACTICE RISK: LAWYERS BEWARE**
BY BRUCE DE'MEDICI
- 18 **MODELING A PRIVACY FRAMEWORK FOR TRUSTWORTHY AI**
BY CHUMA AKANA
- 22 **GENERATIVE AI LITIGATION: A ONE-YEAR CHECK-IN**
BY LUKE RUSHING AND SAMUEL LOWRY
- 26 **USING CHATGPT IN LAW SCHOOL**
BY HARSH MAHAJAN
- 31 **SCITECH NOMINATING COMMITTEE REPORT**
- 34 **GET THE SCITECH EDGE: MEMBERSHIP AND DIVERSITY COMMITTEE NEWS**
BY JOANNE CHARLES
- 35 **FUTURE SCITECH LEADERS: LAW STUDENT ENGAGEMENT COMMITTEE NEWS**
BY DAVID HUSBAND AND CAYLAN FAZIO



AI AND THE COURTS

A LOOK AT THE 2022
NIST-FUNDED AAAS
PROJECT PROVIDING AI
GUIDANCE TO JUDGES

By Alain Norman

Recently, it seems that questions about the use or outputs of artificial intelligence (AI) in the legal field have exploded: When and how should AI be used by lawyers and courts? How trustworthy are AI outputs, and can these be explained? What about possible biases in the data used to develop an AI “tool”? Could AI help with certain types of court proceedings? How might AI relate to jury selection? Could AI someday replace human judges? What is “AI,” anyway?

The American Association for the Advancement of Science (AAAS) undertook a project in 2022 to develop materials for judges on AI. This project, funded by the National Institute of Standards and Technology (NIST), resulted in a number of papers and some podcasts, covering a wide variety of topics, ranging from basic concepts and definitions to how outputs from AI might—or might not—serve as trustworthy evidence under the Federal Rules of Evidence.¹ Given that most of the materials are papers, this article seeks to provide, in writing, the highlights of the three podcasts², generated during the project, that centered around how AI-based tools are being used in the legal profession and how AI could affect decision-making by courts.

AI AND RISK SCORES

Each podcast brought together legal and AI experts,³ who answered questions and engaged in lively discussions. The first podcast looked at “risk scores”—tools that, on the basis of certain criteria, generate probabilities as to the risk of a given person either suffering some harm or engaging in harmful behavior.⁴ Among the key points made by the panelists was that a distinction ought to be made between risk scores that might support the provision of social services and risk scores that might be utilized in the course of legal proceedings, such as pre-trial release or, perhaps, sentencing.

Our experts noted, however, that there is a lack of standards regarding the factors that go into the “secret sauces” of risk scores. At the same time, even if risk scores used in legal proceedings include few factors (vice

risk score formulas used for social service determinations), such factors might inadvertently reflect racial or other biases (e.g., using a person’s zip code can be a proxy for socioeconomic status; also, a person’s arrest record needs to be distinguished from a person’s conviction record, if any).

Panelists underscored that although risk scores—which often are just statistical assessments, not requiring AI—are predictive, a human (e.g., a judge) must still consider the costs and benefits—for the individual and society—of acting upon the risk score in one manner or the other (e.g., pre-trial detention or release). Importantly, work is underway to incorporate “mitigating” factors into risk scores related post-conviction release; such factors might include whether an incarcerated person completed their education, and/or exhibited good behavior, while in jail. Such factors may be termed “dynamic” to reflect whether or how an incarcerated person changed (for the better) over time.

AI IN THE LEGAL PROFESSION

In the second podcast, AAAS brought in persons whose work involves AI tools to help law firms deal with otherwise traditional forms of work, particularly related to litigation, including discovery, assessing the terms and scope of contracts, and developing legal theories or arguments.⁵ Key take-aways from our panelists included that AI is clearly superior to humans at going through vast amounts of information—and doing so more rapidly than humans—to identify patterns that can help firms prepare for litigation. Indeed, lawyers need, as the ABA has long advocated, to maintain “technological competency.” This is likely to include the use of some kind of “technology assisted review” (TAR), to avoid professional malpractice.

Importantly, panelists repeatedly noted that “all major search engines” can handle synonyms. That means these tools are capable of searching for, and identifying, concepts—not just performing keyword searches. To create a simplified example, an AI tool—being used in assisting with “e-discovery”—might not be limited to finding the word

“glad” or “happy” in a mass of data, but rather it might be able to find passages that seem relevant to the concept of joy or satisfaction. Indeed, AI tools can even perform “sentiment analysis,” i.e., help to determine, by evaluating an employee’s emails, whether the person’s messages were likely to be “sarcastic,” “serious,” or something else. This, said the panelists, can be important in flagging potential cases of harassment or misconduct in internal investigations.

Other uses of AI tools—given that they never tire and can rapidly process vast amounts of data to find patterns—include keeping tabs on myriad websites to detect possible violations of intellectual property; keeping abreast of new or changing regulations that might affect a business; reviewing large numbers of contracts to assess the totality of a given company’s contractual obligations; flagging possible plagiarism; and assessing documents and/or legal precedents to help identify new or better lines of argument or bases for litigation.

Yet, our panelists also felt certain that humans remain needed to double-check the results of AI tools. Indeed, humans will remain necessary, particularly for understanding and acting upon subtle, novel, or exceptional issues. As regards how AI tools might affect the future of legal work, companies developing AI “solutions” take the position that AI will help relieve humans (e.g., first-year associates) from “numbing” tasks in order to focus on “higher-value” analysis.

In sum, panelists suggested that some form of “conjoint” or hybrid decision-making is likely to be the best approach. Nevertheless, law firms will have to figure out what constitutes—for them and their clients—the right “mix” of AI and human intelligence to achieve their goals.

Also during the second panel discussion, the question arose of what judges are to make of AI-revealed patterns (from reams of data) that might be offered in support of a given party’s contentions. Put another way, a court might wonder what weight to place on the proffered information or finding, and that, in turn, might depend

on whether the judge seeks to inquire as to how well the data were “coded” in the first place. For companies creating AI tools to assist with document review or data analytics, this becomes a question of “quality management control”—where humans and AI are “pitted” against each other in the process of “training” the AI (or machine learning) tool such that it can achieve a good balance between “over” or “under” capturing seemingly relevant information. This has been termed the “F1” score—the harmonic mean.⁶

Leaving aside the possibility that AI tools might become useful to courts in managing their heavy workflows—in ways perhaps analogous to how law firms incorporate AI into their work, as indicated above—one way that AI-backed search engines are already intersecting courtrooms involves jury selection. That is, services now exist to find and assess the social media history of potential jurors—just as is being done in the context of checking on insurance claims or potential employees. Panelists indicated such probing of potential jurors’ social media presence is, currently, allowed in every jurisdiction, but courts might become concerned about manipulation of the *voir-dire* process and/or individuals’ privacy, over time.

AI AND DECISION-MAKING IN THE JUSTICE SYSTEM

In the third podcast, panelists peered into the future: Will AI replace human judges and/or jurors?⁷ There are three possibilities, broadly speaking: (1) AI-powered systems might replace humans at certain stages of legal proceedings or to perform certain tasks; (2) AI-powered systems might be rejected because of concerns about bias and/or insufficient “explainability” or transparency; or (3) a hybrid approach arises, whereby AI augments humans’ abilities. In this regard, our experts opined, if American judges’ reticence to leverage court-appointed experts were overcome, AI’s ability to analyze vast amounts of data might even help courts to assess the comprehensiveness, if not also accuracy, of testimony from witnesses who are—in our adversarial



system—necessarily prone to provide their otherwise truthful testimony in the light most favorable to one side of a case.

Already, AI-backed tools are being used in connection with aspects of courts’ work. For instance, AI’s capabilities power both legal research and “judicial analytics” (i.e., the thorough review of judges’ rulings and perhaps their social media profiles).⁸ Indeed, the advent of “natural language processing” is powering the ability of law firms to find, e.g., the words that seem most effective in swaying a given judge. Further, algorithms are used to help perform DNA matching—and such tools are regarded as reliable. At the same time, AI might not be able to salvage the trustworthiness of questionable forensic “sciences” such as bitemarks. Certainly, bias in facial recognition systems is already a matter of public debate.

Yet, these examples beg the basic question of whether rules or laws exist that establish whether or when courts should use AI tools in civil or criminal matters. Our experts said that, so far, only “tentative guidelines” seem to have been issued in some jurisdictions, such as the ethical considerations put forth by the Council of Europe. Indeed, as one panelist put it, “Expecting legal systems to foresee when AI should be

used would be ambitious.” Nonetheless, the use of AI seems rampant in the context of administrative adjudications, and the Administrative Conference of the United States has published a report on this.

So, studies are ongoing as to when AI might helpfully replace somebody in the judicial system, given AI’s strengths as regards to “data crunching,” which may facilitate certain types of fact-finding, a traditional function of judges and juries. Yet, challenges exist in trying to assess less numerically based information.

Indeed, a core question that NIST and others seem to wish to have answered is this: Would it be technically possible to build AI tools in such a manner that human values (e.g., justice and equity) are incorporated into those tools? For now, per our panelists, that question is being debated but is not yet answered.

Beyond the possibility that clever developers of algorithms might somehow build desirable values into AI “solutions” for use in legal proceedings, there lies the question of whether people will accept decisions made by machines. The answer to this is also unclear. On the one hand, there may exist a tendency for people to accept “findings” that, because they come from an advanced technology, appear to be more accurate or otherwise “better.” On the other hand, human juries can nullify laws—a power viewed as a notable component of our system of checks and balances—but that is something AI systems would likely prove unable to allow.

Thus, our experts’ discussion indicated only minor disputes—where the facts are agreed upon and/or the financial consequences are relatively modest—will likely prove most amenable to resolution using AI-backed decision-making. Already, AI-facilitated dispute resolution exists in Great Britain, for cases involving amounts capped at £25,000. Also, online dispute resolution (ODR) may have a place in cases where one party (e.g., a tenant) lacks the resources to obtain the assistance of counsel. If people cannot otherwise obtain redress, a system with

little or no human involvement might prove acceptable.

Yet, in “complex” cases—or where the stakes are high or the risk of significant harm in the case of error is high—reliance mainly on AI will probably remain unacceptable. Indeed, even as regards the use of AI tools in “simple” cases, our experts advised that there be mechanisms for appealing AI decisions to a human panel or court. That is because, again, the databases on which such AI systems are built are “noisy”; in computer scientist terms, they are not perfect.

THE RESPONSIBILITY TO PREPARE FOR AI IN THE LAW

Key overall take-aways include the following: AI is very good at analyzing large amounts of data to find patterns, which is something humans do, but which AI tools can achieve much faster; however, AI-revealed “correlations” or predictions do not necessarily constitute proof. Accordingly, humans are, and likely will remain, crucial to making final determinations as to the import or weight of information derived from AI tools. Meanwhile, studies are being conducted at “the nexus of computer and social science” to understand whether, or how, humans and machines might best be combined to achieve optimal “conjoined outcomes.”

Yet, it remains unclear whether or how human “values that are difficult to quantify” (e.g., justice, mercy, or equity) could be incorporated into AI tools. Certainly, NIST has suggested that we are all trying to define and address “socio-technical” challenges arising from the increasing use and sophistication of AI tools.⁹

Indeed, AI’s role in legal proceedings has been, and will remain, complicated by very human limitations and concerns—for instance, certain human values or legal concepts (e.g., “beyond a reasonable doubt”) may be difficult to define; organizations may use an AI tool, designed for one function, in ways for which it was neither designed nor tested (i.e., “mission creep”); and humans often need to be trained on how to use a given AI “solution” and/

or need a better grasp of statistical “uncertainty.” As regards that last point, lawyers and judges would do well, our experts noted, to consider not only the likelihood of an error arising from the use of an AI tool, but also the severity, or nature, of any harm arising from a possible (even if not likely) error.

Notwithstanding the many details to be sorted out, it is clear that AI is being rapidly and increasingly incorporated into legal work, administrative adjudications, and aspects of courts’ work. Accordingly, judges and lawyers must enhance their awareness of the presence, utility, and limitations of various AI tools: By better understanding what such tools can, or cannot, do and by better understanding how the data, development, and deployment of AI-backed tools might be questioned, these instruments can be leveraged responsibly to streamline workflow, identify possible issues or solutions, and—perhaps—contribute to improving the administration of justice.

Alain Norman is an attorney who headed the Science and the Law Initiative of the Center for Scientific Responsibility and Justice at the American Association for the Advancement of Science for the past three years. He served for 22 years as a Foreign Service Officer with the Department of State and inter alia headed a regional office covering 15 countries in Latin America and the Caribbean. Prior to working as a diplomat, Alain established and ran the liaison office of the ABA’s Coalition for International Justice program in The Hague at the International Criminal Tribunal for the former Yugoslavia for three years.

ENDNOTES

1. *Artificial Intelligence and the Courts: Materials for Judges*, AM. ASS’N FOR ADVANCEMENT OF SCI. (AAAS), <https://www.aaas.org/ai2/projects/law/judicialpapers>.

2. AAAS, *Podcast Series: AAAS Artificial Intelligence and the Justice System (2022)*, <https://www.aaas.org/podcast/ai4judges>.

3. Prof. Fredric (Fred) I. Lederer, Chancellor Professor of Law and Director of the Center for Legal & Court Technology (CLCT) at William & Mary Law School, <https://www.legaltechcenter.net/about-us/meet-the-team>; Prof. Iria Giuffrida, Assistant Dean for Academic and Faculty Affairs and Professor of the Practice of Law, at William & Mary Law School, <https://law2.wm.edu/faculty/bios/fulltime/igiuffrida.php>; Prof. Cynthia Rudin, Earl D. McLean Jr. Professor of Computer Science, Electrical and Computer Engineering, Statistical Science, Mathematics, and Biostatistics & Bioinformatics at Duke University, <https://users.cs.duke.edu/~cynthia>; Chris Gottfried, Senior Manager and U.S. Operational Capabilities Lead, at the firm Factor Law, <https://www.factor.law>; and Lisa Prowse, Manager, Relativity Department of Factor Law’s Client Technology Division, <https://www.factor.law>.

4. Podcast Series: AAAS Artificial Intelligence and the Justice System (2022), *Episode 1: AI and Risk Scores*, <https://www.aaas.org/podcast/ai4judges>.

5. Podcast Series: AAAS Artificial Intelligence and the Justice System (2022), *Episode 2: AI in the Legal Field—Commercial and Unexpected Uses*, <https://www.aaas.org/podcast/ai4judges>.

6. On the harmonic mean, see, for example, *F-score*, WIKIPEDIA (Feb. 8, 2024), <https://en.wikipedia.org/wiki/F-score>. For more on how courts might handle such matters, see AAAS, *ARTIFICIAL INTELLIGENCE AND THE COURTS: MATERIALS FOR JUDGES: ARTIFICIAL INTELLIGENCE, TRUSTWORTHINESS, AND LITIGATION* (Sept. 2022), <https://www.aaas.org/ai2/projects/law/judicialpapers>.

7. Podcast Series: AAAS Artificial Intelligence and the Justice System (2022), *Episode 3: AI, Decision-Making, and the Role of Judges*, <https://www.aaas.org/podcast/ai4judges>.

8. For more on both such uses of AI, see AAAS, *ARTIFICIAL INTELLIGENCE AND THE COURTS: MATERIALS FOR JUDGES: ARTIFICIAL INTELLIGENCE, LEGAL RESEARCH, AND JUDICIAL ANALYTICS* (Sept. 2022), <https://www.aaas.org/ai2/projects/law/judicialpapers>.

9. See, e.g., NAT’L INST. OF STANDARDS & TECH., *ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0)* (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.



Navigating the Patchwork of AI Laws, Standards, and Guidance

By Emily Maxim Lamm

The opening weeks of 2024 have seen a record number of state legislative proposals seeking to regulate artificial intelligence (AI) across different sectors in the United States. For example, in light of the upcoming presidential election, a handful of proposals focus on imposing limitations and requirements on the use of generative AI in the context of election campaigns.¹ Meanwhile, on January 8, 2024, Indiana proposed S.B. 7, which would impose prohibitions on the dissemination of media created by generative AI technology, and on January 11, 2024, Georgia proposed H.B. 887, a bill that would prohibit the use of AI in making certain insurance coverage decisions. And several states, including Florida, Kentucky, Virginia, Washington, and West Virginia, have proposed bills creating AI task forces.² At the same time, Congress is facing increased pressure to pass AI legislation to tackle an array of potential risks, particularly in light of recent media firestorms surrounding deepfakes of celebrities and robocalls impersonating presidential candidates.

With this type of rapid-fire start to the 2024 legislative season, the AI legal landscape will likely continue evolving across the board. As a result, organizations today are facing a complex and dizzying web of proposed and existing AI laws, standards, and guidance.

This article aims to provide a cohesive overview of this AI patchwork and to help organizations navigate this increasingly intricate terrain. The focus here will be on the implications of the White House AI Executive Order, existing state and local laws in the United States, the European Union's AI Act, and, finally, governance standards to help bring these diverse elements together within a framework.

THE AI EXECUTIVE ORDER

On October 30, 2023, the Biden administration took a monumental step in releasing the Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (the AI Executive Order).³ This landmark AI Executive Order leverages the federal government's significant role as a

purchaser of AI software and hardware to establish guardrails and requirements regarding the development and deployment of AI. The 111-page order encourages the use of AI throughout the government, directing federal agencies to issue guidance in the forthcoming months.

The Department of Labor, for instance, is directed to “develop and publish principles and best practices for employers that could be used to mitigate AI’s potential harms to employees’ well-being and maximize its potential benefits.” Although simply guidance, these best practices and principles regarding AI in employment likely provide insight into how the agency will approach AI-related enforcement actions in the future. Meanwhile, the AI Executive Order tasks the Secretary of Commerce with requiring companies developing dual-use foundation models to report ongoing or planned activities related to training, development, or production of such models. U.S.-based Infrastructure as a Service providers are also required to submit reports to the Secretary of Commerce when a foreign person transacts with them to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. In addition, the AI Executive Order requires the Secretary of Commerce for Intellectual Property and Director of the U.S. Patent and Trademark Office to develop guidance on inventorship, patent eligibility, treatment of copyrighted works in AI training, and the scope of protection for works produced using AI and the use of copyrighted works in AI training. The AI Executive Order also builds on the White House’s Voluntary AI Commitments,⁴ including by tasking the National Institute for Standards and Technology (NIST) with the development of guidelines for performing AI red-teaming (i.e., structured adversarial testing) of foundation models.⁵

While the AI Executive Order is primarily focused on the federal government and those developing the most potent AI systems, the standards it creates are likely to impact organizations in the private sector. This is especially the

case given that the federal government is already a significant AI consumer, which will inevitably influence how vendors with government procurement arms will develop their AI systems. Notably, the White House’s Office of Management and Budget (OMB) issued draft guidance to the federal government regarding its own use of AI, which may have a precedential impact on other legislation coming down the pipeline.⁶ The OMB draft memorandum focuses upon safety- and rights-impacting AI systems (i.e., systems with consequential and significant effects) and proposes requirements with respect to opt-out rights, notification, and impact assessments, among others.

EXISTING PATCHWORK OF U.S. AI LAWS

Amid these national developments, existing U.S. state and local laws, especially in New York City, Illinois, Maryland, Colorado, and California, contribute to the AI regulatory compliance headache for organizations.

In the context of AI in the workplace, there are three existing laws with a focus on hiring. First, Illinois regulates the use of AI video interview analysis by imposing advanced notice requirements about the use of AI and how it works, requiring consent from applicants, and providing applicants with the right to request that their video interview be deleted.⁷ Illinois also imposes data collection and reporting requirements on employers solely relying upon AI video analysis to determine if an applicant is selected for an in-person interview. Similarly, Maryland requires employers to obtain consent for the use of facial recognition services in applicant interviews.⁸ Meanwhile, on July 5, 2023, New York City’s Department of Consumer and Worker Protection began enforcing Local Law 144, the broadest law governing AI in employment in the United States.⁹ Local Law 144 prohibits employers from using an automated employment decision tool (AEDT) in hiring and promotion decisions *unless* it has been the subject of an annual bias audit based on race, sex, and ethnicity by an “independent auditor” no more than one year prior to use. The

law also imposes certain posting and notice requirements to applicants and employees who are subject to the use of an AEDT.

Further, when deploying AI systems in the workplace, data privacy laws also must be taken into account. As of January 1, 2023, the personal information of employees, job applicants, and independent contractors became subject to the California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA).¹⁰ Under the CPRA, employers must provide notice about the collection of employment-related personal information, how that data are used, and the period for which the data will be retained, among other requirements. Meanwhile, Illinois’s Biometric Information Privacy Act requires informing individuals that a biometric identifier (e.g., a fingerprint or retina scan) or biometric information is being stored or collected, obtaining a written release from the individuals subject to the storage or collection, and publishing a written policy with a retention schedule and guidelines for destroying biometric identifiers and information.

In a different sector, the Colorado Division of Insurance implemented a final regulation, effective on November 14, 2023, requiring life insurers operating in Colorado to integrate AI governance and risk-management measures.¹¹ Under these regulations, insurers must remediate any instances of detected unfair discrimination, conduct a comprehensive gap analysis and risk assessments, and comply with documentation requirements, including maintaining an up-to-date inventory of AI models, documenting material changes, bias assessments, ongoing monitoring, vendor selection processes, and annual reviews.

With the slew of sector-specific AI proposals across state legislatures, this patchwork is likely to continue growing.

GLOBAL IMPLICATIONS OF THE EU AI ACT

Moving beyond U.S. borders, the European Union’s Artificial Intelligence Act (EU AI Act) stands out as a pioneering effort in comprehensive AI legislation.

On December 8, 2023, EU legislators reached a political agreement on the EU AI Act,¹² and on February 2, 2024, the member states of the EU unanimously voted to move forward with it.¹³ The EU AI Act's comprehensive legislative framework aims to regulate AI across sectors and industries and, given its extra-territorial effect, may have far-reaching implications for organizations globally if they do business in the EU. The EU AI Act takes a risk-based approach to legislation, establishing requirements for AI depending on its level of impact on fundamental rights and potential risk.

An AI system is categorized as “high risk” if it poses a significant risk to an individual's health, safety, or fundamental rights and is used, or intended to be used, in certain critical areas, such as employment, public services, education, critical infrastructure, law enforcement, border control, and the administration of justice. High-risk systems are subject to an array of compliance obligations, including technical documentation, data governance, human oversight, recordkeeping, conformity assessments, a risk management system, post-market monitoring, and fundamental rights impact assessments. So-called general purpose AI (GPAI) models (i.e., foundation models) posing a systemic risk—presumed when trained using a total computing power of more than 10^{25} floating point operations—are subject to additional rules, including model evaluations, adversarial testing, mitigating of systemic risk, and reporting on energy efficiency. The EU AI Act also prohibits certain AI systems posing an “unacceptable” risk (e.g., AI used to exploit the vulnerabilities of people) while imposing transparency requirements on those presenting a low risk.

The EU AI Act's requirements will go into effect through a staggered schedule. After entry into force, its obligations will apply six months after for prohibited AI, 12 months after for obligations for GPAI/foundation models, 24 months after for Annex III high-risk requirements, and



36 months after for Annex II high-risk requirements.

The EU General Data Protection Regulation (GDPR) is another layer to keep in mind in the context of the forthcoming EU AI Act.¹⁴ For example, Article 22 of the GDPR applies to decisions based *solely* on automated processing, including profiling, that produce legal or similarly significant effects on an individual and requires such decisions to only be taken based on contractual necessity, explicit consent, or where authorized by an EU or member state law. Notably, a recent decision from the European Court of Justice applied Article 22 to instances in which automated credit scoring was allegedly used to automatically reject loan applications.¹⁵ In addition, the GDPR imposes several risk mitigation requirements on data controllers, including implementing data protection policies and conducting data protection impact assessments. Although the GDPR is, of course, narrower in scope than the EU AI Act, organizations that

have already developed procedures and structures to comply with the GDPR will be able to leverage and expand upon them to comply with the EU AI Act's data governance and impact assessment requirements.

AI GOVERNANCE STANDARDS: NIST AND ISO 42001

Now that we've made our way through the many laws governing AI in different jurisdictions and sectors, you might be wondering how it's possible to make sense of all of these concepts and fit the requirements together in a practical manner. This is where AI governance comes in. Admittedly, AI governance sometimes seems like a bit of an amorphous concept filled with fluffy buzzwords detached from practicality. However, implementing an effective AI governance system is ultimately the glue for an organization to be able to navigate and comply with this intricate regulatory landscape. Several leading organizations have remained at the forefront of this area and have developed tools to help organizations implement a governance plan.

On January 26, 2023, NIST issued the voluntary Artificial Intelligence Risk Management Framework 1.0 (AI RMF).¹⁶ In the absence of a mandatory regulatory framework in the United States—and with the threat of litigation and regulatory inquiries looming—a growing consensus arose around its emergence as the central risk-based framework for building AI compliance programs that incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, systems, and services. Indeed, NIST is no stranger to such reach—NIST's Cybersecurity Framework issued in February 2014 has become the global standard for cybersecurity practices in the absence of federal regulation. NIST's AI RMF provides guidelines for building AI compliance programs that incorporate trustworthiness and transparency considerations across the AI life cycle, including practical guideposts such as conducting risk assessments and audits.

The International Organization for Standardization's (ISO) 42001 is an international standard that outlines another voluntary framework for establishing and maintaining an AI management system that ensures responsible development and deployment of AI within organizations.¹⁷ Like NIST's AI RMF, ISO 42001 is intended for organizations of any size and is applicable across industries. Instead of imposing rigid definitions or requirements, ISO 42001 describes a coherent approach for policies, documentation, and risk management practices and controls. For example, under Sections A.9.2 and A.9.3, ISO 42001 imposes broad obligations on organizations to define processes for the responsible use of AI systems. In contrast, the EU AI Act specifies concrete practices that would fall under responsible AI use, such as listing prohibited AI practices/uses, transparency/notification obligations on deployers/users, and instructions for use.

Accordingly, both NIST's AI RMF and ISO 42001 provide an umbrella within which an organization can develop a unified compliance plan by incorporating applicable legal requirements under the EU AI Act, existing U.S. state and local laws, and potentially forthcoming AI laws and regulations.

* * *

As AI regulations evolve globally, organizations must adopt a harmonized approach to compliance. The interplay between U.S. executive orders, EU legislation, and state and local laws necessitates a comprehensive understanding of AI governance standards. NIST's AI RMF and ISO 42001 offer practical frameworks, guiding organizations through the complex web of AI regulations to facilitate responsible and ethical AI development and deployment.

Emily Maxim Lamm is an attorney at Gibson, Dunn & Crutcher LLP. Her practice has a dual focus on artificial intelligence matters and employment litigation, counseling, and investigations. The views and opinions expressed in this article are those of

the author and do not necessarily reflect the opinions, position, or policy of Gibson, Dunn & Crutcher LLP, or their other employees, affiliates, or clients. The information provided in this article is not, is not intended to be, and shall not be construed to be either the provision of legal advice or an offer to provide legal services. The content here is intended as a general overview of the subject matter covered. Gibson, Dunn & Crutcher LLP is not obligated to provide updates on the information herein. Those reading this article are encouraged to seek direct counsel on legal questions.

ENDNOTES

1. See, e.g., 2023 H.S.B. 599 (Iowa Jan. 23, 2024); 2023 H.B. 2559 (Kan. Jan. 22, 2024); 2024 H.B. 182 (N.M. Jan. 22, 2024).

2. 2024 Fla. H.B. 1459; 2023 Ky. H.C.R. 38; 2024 Va. S.B. 621; 2024 Wash. S.B. 6184; 2024 W.Va. H.R. 3.

3. The White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, BRIEFING ROOM (Oct. 30, 2023), <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>.

4. Press Release, The White House, Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai>.

5. NIST issued a request for information on December 19, 2023. See *NIST Calls for Information to Support Safe, Secure and Trustworthy Development and Use of Artificial Intelligence*, NIST (Dec. 19, 2023), <https://www.nist.gov/news-events/news/2023/12/nist-calls-information-support-safe-secure-and-trustworthy-development-and>.

6. Proposed Memorandum from Shalanda D. Young, OMB, for Heads of Exec. Depts & Agencies, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (Oct. 30, 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf>.

7. 820 ILL. COMP. STAT. ANN. § 42.

8. MD. CODE ANN., LAB. & EMPL. § 3-717.

9. N.Y.C., INT. 1894-2020, LOCAL LAW 144, <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9>.

10. *California Consumer Privacy Act (CCPA)*, CAL. DEP'T JUST., <https://tinyurl.com/ms6y4muy> (updated May 10, 2023).

11. Press Release, Colo. Div. of Ins., Notice of Adoption—New Regulation 10-1-1 Governance and Risk Management Framework Requirements for Life Insurers' Use of External Consumer Data and Information Sources, Algorithms, and Predictive Models (effective Nov. 14, 2023), <https://doi.colorado.gov/announcements/notice-of-adoption-new-regulation-10-1-1-governance-and-risk-management-framework>.

12. Press Release, European Parliament, Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI (Dec. 9, 2023), <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligenceact-deal-on-comprehensive-rules-for-trustworthy-ai>.

13. Jedidiah Bracy & Caitlin Andrews, *EU Countries Vote Unanimously to Approve AI Act*, IAPP (Feb. 2, 2024), <https://iapp.org/news/a/eu-countries-vote-unanimously-to-approve-ai-act>.

14. General Data Protection Regulation, 2016/679, <https://gdpr-info.eu>.

15. Case C-634.21, *OQ v. Land Hesse (SCHUFA Holding AG)*, EU:C:2023:957 (Dec. 7, 2023), <https://tinyurl.com/4ketpprj>.

16. NIST, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

17. ISO/IEC 42001:2023, <https://www.iso.org/standard/81230.html>.



Deepfakes and Malpractice Risk: Lawyers Beware

By Bruce de'Medici



Advances in artificial intelligence (AI) are making it easier than ever to create hyper-realistic fake audio and video, known as “deepfakes.” While deepfakes can enable creative new forms of expression, they also pose serious professional liability risks that could lead to ethical or malpractice claims, and other sanctions, if attorneys fail to exercise reasonable care.

WHAT ARE DEEPFAKES AND WHY DO THEY MATTER?

Deepfakes leverage powerful machine learning (ML) techniques to swap one person’s face or voice onto video or audio of someone else or create other inauthentic results. The resulting fabricated media can appear strikingly authentic and can be used to present false portrayals that threaten business loss or personal setbacks.

Lawyers may encounter deepfakes/potential deepfakes in various settings, including:

- evidence in administrative and judicial forums;
- defamation attacks;
- support for insurance claims; or
- support for commercial ransom demands (threats to circulate imagery that impacts commercial enterprise value—e.g., imagery representing a C-suite member in a meeting with competitors or prohibited foreign actors).

In September 2023, the NSA, FBI, and CISA issued a Cybersecurity Information Sheet in which they listed deepfakes as making the list of top risks for 2023.¹ In its *The Global Risks Report 2024*,² the World Economic Forum ranked “misinformation and disinformation” as presenting the highest “likely global impact (severity)” over a two-year period³ and the second-highest risk “likely to present a material crisis on a global scale in 2024.”⁴ Estimates of deepfakes in circulation online vary.⁵ The foregoing represent evidence of an increasing frequency of deepfakes in existence and an increasing

probability of them intersecting a lawyer’s practice.

WHY WE CAN’T RELY ON OUR EYES TO DETECT DEEPFAKES

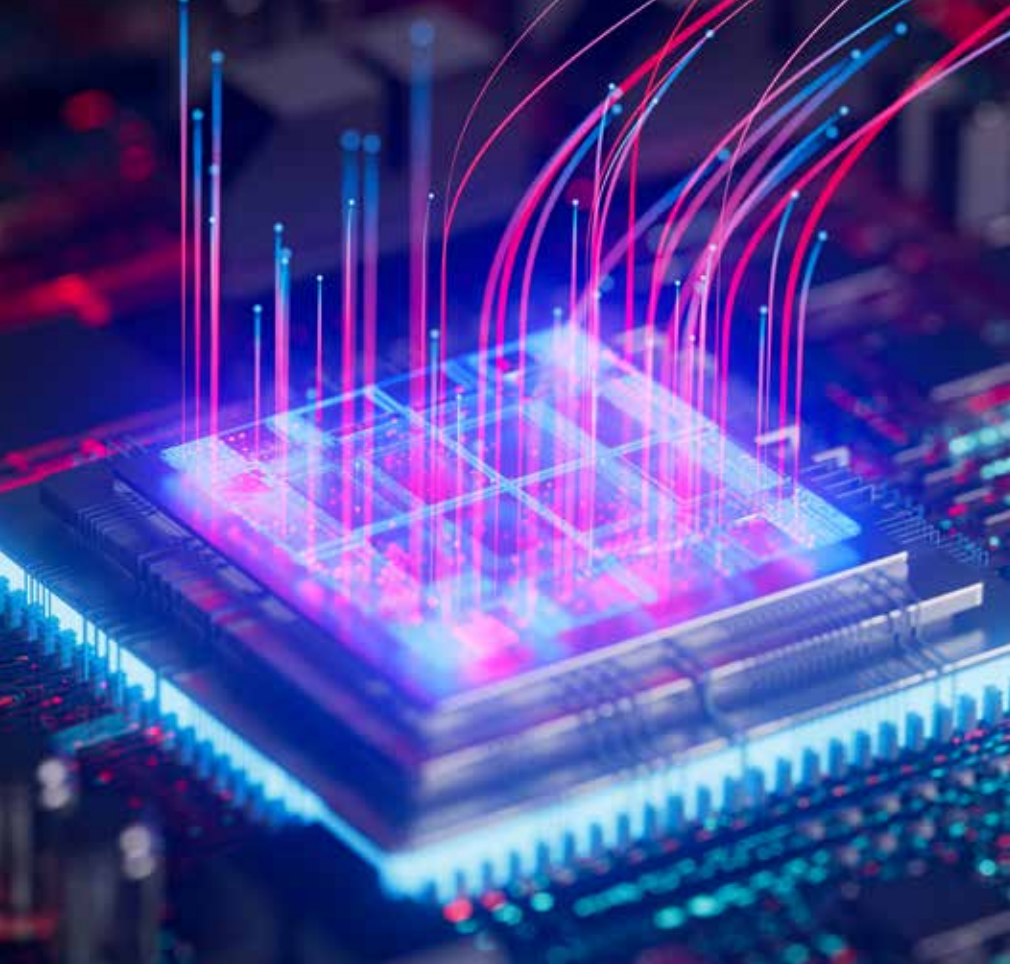
The human eye is increasingly unable to spot deepfake manipulations. Developers leverage the same AI that enables doctored media to systematically defeat human detection. They train deep learning models called “generative adversarial networks,” where two neural networks face off—one generates fabricated images or audio while the other tries to identify them as fake. This adversarial back-and-forth progressively improves the generator’s ability to create realistic fakes and teaches it to avoid telltale signs that humans can detect. The results are persuasively realistic deepfakes that fool most people. In tests, humans spotted deepfake videos just over half the time—barely better than a coin flip. Detection rates can be even worse for doctored audio. Our eyes and ears cannot keep pace with AI’s rapid advances.

It is tempting to expect that lawyers can reliably detect doctored evidence just as they can catch a witness in a lie during cross-examination. But deepfakes are increasing in sophistication and becoming increasingly difficult to detect. Unless lawyers stay informed on the state of the art in deepfake generation, they risk allowing manipulated materials to improperly influence their advice and advocacy.

DEEPFAKE DETECTION—A TECHNOLOGY ARMS RACE

Fortunately, the same ML techniques used to create deepfakes can also detect them. AI-powered forensic analysis can spot subtle manipulation clues imperceptible to humans. But deepfake generation models continually evolve to sidestep detection by AI watchdogs.

This technical arms race means AI detection requires constant upgrading to analyze the latest manipulation methods. Static analysis tools will inevitably fall behind state-of-the-art deepfake creation technologies. Only dynamic detection models that



continually learn to find new manipulation fingerprints can keep pace as deepfake creators invent new tricks.

Humans must partner with evolving AI detectors to reliably confirm evidence integrity. We can no longer trust our naked eyes as definitive arbiters of reality in the face of AI-doctored content. Only vigilant human-machine teamwork has a chance of piecing digital truth from well-disguised lies.

AI TECHNIQUES FOR CREATING HYPER-REALISTIC DEEPAKES

Machine learning is a subset of AI—the learning occurs by fitting mathematical models to observed data. It involves the development and evaluation of algorithms that enable a computer to learn patterns from one or more sets of data. It enables data-driven decisions through identifying and extracting patterns from sets of data that, in turn, map from sets of complex inputs into good decision outcomes.

An algorithm is a mathematical formula that a computer can understand and that instructs a computer to analyze set(s) of data and identify recurring

patterns or relationships within the data. An ML algorithm is a search process with the (user's) purpose being to choose the function (from a set of possible functions) that explains relationships between features in data in a fashion that meets the user's needs. A function specifies a class of problems that can be modeled and solved (or not solved)—a deterministic mapping of input values (applied to the data) and resulting output values. Computers perform this process within sets of data that people cannot practically process themselves.

Algorithms can be both “rules-based” (written to search for particular patterns) or agnostic (written to allow the data to reveal patterns that are not specified or queried in the algorithm). At a sophisticated level, an agnostic algorithm allows data to “speak” on their own and identifies patterns in data that are not known prior to applying the algorithm. In mathematical terms, these patterns of relationships are functions. An example could be a pattern relating income and debt level to credit rating.

The patterns that deep learning algorithms extract from data are functions that are represented as neural networks.

In simplified terms, a neuron accepts certain values as inputs and maps them to an output value. In a network, the output value of a neuron is passed on as input to the next neuron. Each neuron learns a simple function—the more complex function is created by combining the neurons (and the learning process) in the network. The structure of the network defines the more complex function. A deep neural network is a type of model used in ML that is loosely inspired by the structure of the brain and capable of making accurate data-driven decisions.

Deep learning focuses on deep neural network models and fits them to data. Again, deepfakes can be constructed from utilizing deep learning.

Generative Adversarial Networks

The most common approach to generating deepfakes is using a class of AI models called generative adversarial networks (GANs). GANs leverage two neural networks—a generator and a discriminator. The generator creates fake images or videos that seem real, while the discriminator tries to identify fakes. Playing this minimax game drives the generator to create more and more realistic fakes that can get past the discriminator.

The training process of GANs can be framed as a supervised learning problem, where the generator and discriminator are trained together. The goal is to train the generator to produce plausible examples that can fool the discriminator, while the discriminator aims to become better at distinguishing between real and fake examples.

GANs are often used with image data and employ convolutional neural networks (CNNs) as the generator and discriminator models. They have been successfully applied in various computer vision tasks, such as generating realistic-looking images, deepfakes, and image-to-image translation.

Convolutional Neural Networks

A CNN is a type of a neural network that takes additional contextual or conditional input to guide its productions of outputs.

A CNN has three types of layers:

- The *convolutional layer* is the core building block of a CNN and is where the majority of the computation occurs. It applies filters to the input image to extract features, such as edges and shapes.
- The *pooling layer* down-samples the image to reduce computation and extract the most important features.
- The *fully connected layer* makes the final prediction by taking the output of the previous layers and mapping it to a class label.

CNNs are particularly useful for finding patterns in images to recognize objects, classes, and categories. They can also be quite effective for classifying audio, time series, and signal data. CNNs can have tens or hundreds of layers, with each learning to detect different features of an image. The filters can start as very simple features, such as brightness and edges, and increase in complexity to features that uniquely define the object. With each layer, the CNN increases in its complexity, identifying greater portions of the image.

Applications of GANs

- *Generate Photographs of Human Faces:* GANs generate realistic photographs of human faces, which can be useful in various applications, including advertising, gaming, and virtual reality.
- *Image-to-Image Translation:* GANs translate images from one domain to another, such as converting a sketch into a realistic image or transforming a daytime image into a nighttime scene.
- *Text-to-Image Translation:* GANs generate images based on textual descriptions, allowing users to create visual content by simply describing it in words.
- *Face Frontal View Generation:* GANs generate frontal views

of faces based on side or angled images, which can be useful in entertainment, security, and surveillance applications.

- *Video Prediction:* GANs predict future frames in a video sequence, which has applications in autonomous driving, surveillance, and video compression.
- *3D Object Generation:* GANs generate 3D objects based on 2D images or sketches, which can be useful in architecture, product design, and virtual reality.

Autoencoders

Autoencoders are another popular technique for creating deepfakes. These are neural networks that encode input data into a compact representation and then reconstruct the output from this representation. Trained on many images of a person's face, autoencoders can decode new images showing that face from any input image. This enables face-swapping onto target videos. Unlike GANs, autoencoders are not adversarial and consist of two main components, an encoder and a decoder. The encoder compresses the input data into a lower-dimensional representation, while the decoder reconstructs the original input from the compressed representation.

Autoencoders can be trained in an unsupervised manner, where the goal is to minimize the reconstruction error between the input and the output. They are often used for tasks such as anomaly detection, denoising, and dimensionality reduction.

In the context of generative modeling, autoencoders can be used to generate new examples by sampling from the learned latent space. However, they are generally not as effective as GANs in generating high-quality and realistic examples.

Applications of Autoencoders:

- *Anomaly Detection:* Autoencoders can detect anomalies in data by reconstructing input samples and comparing them to the original data. This has applications in fraud detection, network security, and predictive maintenance.

- *Data Compression:* Autoencoders can compress and decompress data, which can be used for tasks such as image and video compression, improvement of transmission efficiency, and reduction of storage requirements.
- *Feature Extraction:* Autoencoders can learn compact representations of input data, useful for tasks such as image recognition, text classification, and recommendation systems.
- *Image Denoising:* Autoencoders can remove noise from images by learning to reconstruct clean versions of the input data. This has applications in medical imaging, photography, and satellite imaging.
- *Dimensionality Reduction:* Autoencoders can reduce the dimensionality of input data while preserving important features, making them useful for classification tasks, clustering, and visualization.

Other Techniques

- *StyleGANs:* Nvidia researchers developed StyleGANs that generate highly realistic synthetic faces by separately controlling attributes like expression, facial structure, hairstyle, and pose. Manipulating these stylistic attributes enables forming a detailed fake face.
- *Face Parsing & Blending:* Other techniques analyze facial geometry in source and target videos to parse angles, face structure, lighting, and skin tones. Advanced blending algorithms then integrate parsed face elements from the source onto the target seamlessly.
- *Voice Cloning:* By manipulating audio, including speech, and leveraging varieties of autoencoders, GANs, and style transfer techniques, the resulting voice cloning can mimic target vocal mannerisms and statements.

AI AND QUANTUM COMPUTERS

As a general description, quantum computing is predicated upon the laws of quantum mechanics (that physics works differently at an atomic scale and a sub-atomic scale). Efforts to operationalize quantum computing are ongoing and operationalization at either full or limited capacity will plausibly occur within less than 10 years. NIST has announced that it is “critical” to begin planning now for the decryption threat of quantum computing.⁶ In the mean, experts predict that market impact of quantum computing will be over \$4 billion by 2029, and McKinsey predicts \$106 billion market impact by 2040.

AI will empower quantum computing and be hugely augmented by quantum computing. “Quantum AI” is presently moving at a pace and in a direction for results that many experts suggest “natural” intelligence may not be capable of controlling, predicting, or understanding.

Quantum AI will empower creation of ever sophisticated deepfakes in minutes or even seconds. A quantum AI-driven computer could generate orders of magnitude more sophisticated deepfakes than are presently achievable. In short, sophisticated deepfakes threaten to become commonplace in business and personal lives; effectively addressing them will become an indispensable requirement for the competent practice of law and competing in the marketplace.

PROACTIVE EFFORTS TO TAME DEEPFAKES

Any future legislation concerning deepfakes would be directed toward reducing uncertainty and risk in this landscape and would need to address the ongoing and fast-paced advancements in AI and related technology. The landscape on deepfake detection is presently similar to the adversarial chase in cybersecurity, whereby advances in cyber hygiene and detection offer varying levels of risk management or reduction, but continuing evolution in cyberattack techniques imposes a temporality to any remedial technique.

For example, detection techniques usually rely on deep learning classifiers to determine if a visual media image



is fake or real. Adversarial techniques work against this detection methodology—deepfake creators with knowledge of detection technology can insert slight “perturbations” and noise to the deepfake images to modify the deepfake generation pipeline and exploit blind spots in the detection models. This can cause the deepfake classifier to inaccurately characterize a deepfake as authentic. Examples of these perturbations and noises are pixel-level attacks (direct modification in the images through Gaussian noise, changes to pixel intensities, or flipping low-bit pixel images) and spatial transformations (manipulation of the geometry of images by, e.g., shifting them in position, rotating the images, or enlarging/shrinking dimensions in the images, mixing with out-of-distribution images, or adding near-invisible pixels from other images). These perturbations and noise are sufficient to fool detection models and are invisible to the human eye.

Pending a breakthrough in detection architecture, best practice is to assume that any remedial deepfake detection technique has limits on effectiveness, in both scope and temporal longevity. Maintaining a sharp eye on these limits will be key to effective deepfake detection hygiene.

DUTIES AND RISKS

Attorneys Have an Ethical Duty to Understand Deepfakes

A number of the ABA Model Rules could be potentially invoked in connection

with a lawyer encountering deepfakes in a law practice. Examples include the following:

Rule 1.1: Competence—sufficient knowledge, preparation, skill, and thoroughness that is reasonably necessary for the representation.

Rule 3.1: Meritorious Claims and Contentions—diligence that a claim or defense has a basis in fact.

Rule 3.3: Candor toward the Tribunal—not offering evidence that the lawyer knows to be false.

Rule 3.4: Fairness to Opposing Party and Counsel—not alluding to any matter that the lawyer does not reasonably believe is relevant or that will not be supported by admissible evidence.

Rule 4.1: Truthfulness in Statements to Others—not making a false statement of material fact or law to a third person.

Rule 8.3: Reporting Professional Misconduct—potential reporting if a lawyer engages in unprofessional conduct regarding a deepfake.

Potential Ethical Challenges

Lawyers who ignore how deepfakes enable new forms of deception may lack the requisite technological knowledge to represent clients diligently, as required by Model Rule 1.1. Similarly, allowing deepfakes to mislead you or your clients could also run afoul of ethics rules on truthfulness. Under Model Rule 4.1, lawyers cannot knowingly make a false statement of material fact to a third person. An attorney fooled by a deepfake risks unwittingly passing

along false information supplied by a client or contained in evidence. Raising a lack of knowledge in the face of an ethical inquiry may invite scrutiny of the lawyer's due diligence in connection with media that turned out to be a deepfake.

Parties could also assert "fraud on the court" if an attorney introduces fabricated materials as real evidence or relies on deepfakes without appropriate scrutiny. Such fraud enables sanctions like dismissing cases and assessing attorney fees.

Potential Evidentiary Admission Challenges

Courts may commence conducting pretrial evidentiary hearings on admissibility of audio and visual media. Sensibly, these hearings should occur in coordination with completion of discovery. Best practices may militate in favor of presenting expert witnesses for both proffers to admit media into evidence and rebuttals to contest opponent's proffers. Depending upon the array and technology underlying the media, counsel may engage more than one expert (who would testify respectively as to media structured upon different technology).

Selection of experts for these purposes will require care: Diverse methods are employed to create deepfakes and, as noted above, technology for uncovering skillful deepfakes will vary according to the technology utilized in creating them. As creation technology continues to evolve, best practice calls for counsel attending to whether experts (and their technology focus) are qualified to address the media at stake in the matter at hand. In a word, the expert who carried the day in a recent matter may not be qualified to address the technology at play in the matter at hand.

Counsel would be well-advised to review and tailor their engagement letters or disclosures to clients to address the need to conduct due diligence on media presented by clients for admission. Clients may seek to obtain advantages in legal matters by utilizing deepfakes or obtain media from third parties and be reluctant to test its veracity, especially if the media promise to be persuasive to a trier of fact.

Similarly, counsel may decide to press for costs incurred to rebut an opponent's proffer of a deepfake. As the creation technology progresses, expert costs for uncovering them may correspondingly increase. Thus, the risk of cost sanctions threatens to advance, both in the complexity required in due diligence and the increasing costs required to rebut them.

Potential Malpractice Claims

Beyond disciplinary actions for ethics violations, attorneys' failure to understand deepfakes poses significant malpractice liability. A lawyer could face negligence claims for letting deepfakes distort their legal advice or diligence in reviewing evidence. Further, by advancing arguments based on deepfakes they should have known were likely manipulated, lawyers risk making factual misrepresentations that support malpractice suits.

THE BOTTOM LINE: LAWYERS MUST STAY VIGILANT AGAINST DEEPFAKES

Deepfakes raise novel challenges at the intersection of ethics, law, and technology. Attorneys have professional and ethical duties to understand deepfakes and guard against being misled or allowing deepfakes to mislead others. In light of the new credibility questions introduced by this technology, lawyers who ignore or downplay the risks posed by synthetic media ignore this obligation at their peril. Best practice is to stay informed on deepfake detection best practices and treat digital evidence with caution.

Remaining informed presents an informational challenge. As deepfake technology evolves, so to will the requisite level of knowledge to address them. This knowledge requirement will advance in terms of both quantity (expanding quantity of creation techniques will engender an expanding body of information to absorb) and sophistication (advancing skill in respective creation techniques will engender increasing complexity in understanding them). Maintaining competence in this expanding knowledge will require a corresponding commitment of time.

Counsel would be well-advised to decide whether to rely upon their own knowledge to address the foregoing or engage outside consultants. Counsel should also structure client disclosure and consent on this decision. Deepfakes are an existing component of the present and future risk landscape that lawyers are retained to address. Proactive measures to address the risk are ethically and professionally required.

Bruce de'Medici is the principal of Grey Oar, focusing on advising on the intersection of the commercial application of burgeoning technology and risk. He brings his legal background in commercial litigation and transactions to bear in navigating risk management for enterprises applying AI and other technology for commercial gain.

ENDNOTES

1. Nat'l Sec. Agency, Fed. Bureau of Investigation & Cybersecurity & Infrastructure Sec. Agency, *Contextualizing Deepfake Threats to Organizations*, CYBERSECURITY INFO. SHEET (Sept. 2023), <https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF>.
2. WORLD ECON. F., *THE GLOBAL RISKS REPORT 2024* (Jan. 2024), https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.
3. *Id.* at 9.
4. *Id.* at 13.
5. HOME SEC. HEROES, *2023 STATE OF DEEPFAKES: REALITIES, THREATS, AND IMPACT*, <https://www.homesecurityheroes.com/state-of-deepfakes/> (last visited Jan. 14, 2024) (asserting discovery of 95,820 deepfakes videos online); SUMSUB, *IDENTITY FRAUD REPORT*, https://sumsub.com/fraud-report-2023/?utm_source=pr&utm_medium=article&utm_campaign=fraud_report2023 (last visited Jan. 14, 2024) (asserting a tenfold increase in the number of deepfakes detected worldwide from 2022 to 2023).
6. *Migration to Post-Quantum Cryptography*, NIST: NAT'L CYBERSECURITY CTR. OF EXCELLENCE, <https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms> (last visited Jan. 14, 2024).



Modeling a Privacy Framework for Trustworthy AI

By Chuma Akana



In October 2023, the U.S. president signed an Executive Order focused on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI). The order recognizes the potential of responsible AI to help solve urgent challenges and outlines eight guiding principles and priorities for trustworthy AI, which include ensuring the safety and security of AI and protecting the privacy and civil liberties of Americans.¹ In the same vein, the National Security Telecommunications Advisory Committee (NSTAC) has proposed that by 2028, Americans should be able to rely on technological advancements to protect their privacy and ensure the safety and security of their data.² As AI advances, it has the potential to analyze personal information in new and more intrusive ways, posing a threat to privacy. However, there are proposals to implement privacy protection in AI design, and this article asserts that trustworthy AI demands specific privacy laws. AI is responsible for collecting and analyzing massive amounts of data. Nowadays, many privacy-sensitive activities such as search algorithms, recommendation engines, and ad tech networks rely on machine learning (ML) and algorithmic decision-making. Therefore, it is crucial to have a privacy framework that is specifically designed to address the challenges posed by AI.

In this age of generative AI and ML, it is important to make use of the benefits of technology while also ensuring that there is adequate protection of privacy for users. The National Institute of Standards (NIST) provides guidelines for AI trustworthiness, which include accuracy, explainability and interpretability, privacy, reliability, robustness, safety, security, and the mitigation of harmful bias.³ It is also important that diversity, equity, inclusion, and accessibility are prioritized throughout the entire process of designing, developing, implementing, iterating, and monitoring of AI systems.

AI systems, particularly those utilizing ML, can operate in complex and opaque ways, which make it challenging for individuals to understand

how decisions are made about them. However, data governance is crucial in achieving trustworthy AI, as the full pipeline development and implementation of every AI system must be considered. This includes the objectives for the system, how the model is trained, what privacy and security safeguards are needed, and what the implications are for the end user and society. Furthermore, explaining what training data and features have been selected for an AI system and whether they are appropriate and representative of the population can help counteract common types of AI bias/fairness. Therefore, issues like complex decision-making, data minimization, bias and fairness, explainability, and cross-border data should be taken into consideration while developing AI systems.

PRIVACY FOR TRUSTWORTHY AI

The NIST Artificial Intelligence Risk Management Framework emphasizes the importance of privacy values such as anonymity, confidentiality, and control in guiding choices for AI system design, development, and deployment. Privacy-related risks can affect security, bias, and transparency, and there may be trade-offs between these characteristics. Similar to safety and security, specific technical features of an AI system can either promote or reduce privacy. Furthermore, AI systems can pose new risks to privacy by enabling inference to identify individuals or previously confidential information about them.⁴

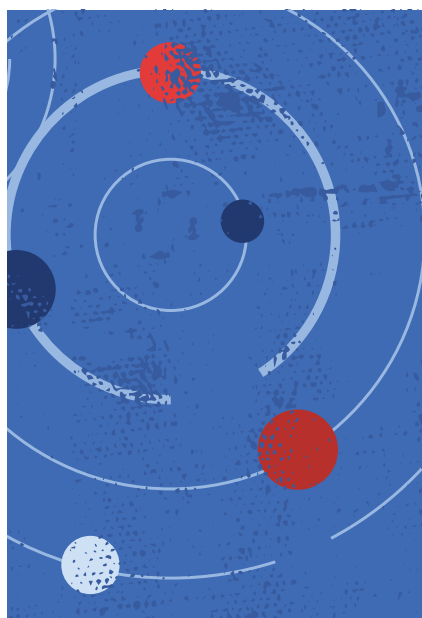
In an attempt to regulate AI with data privacy law, the authors of the California Privacy Rights Act borrowed language on “automated decision-making” (ADM) technologies directly from the General Data Protection Regulation (GDPR). As defined by the GDPR, ADM technologies are those that have “the ability to make decisions by technological means without human involvement,” and the GDPR gives consumers the right to refuse to be subject to any such automated decision insofar as it produces legal consequences. While ADM is not synonymous with AI (ADM is rule-based and follows predetermined instructions, while AI can learn from

data and make decisions based on those data), a broad range of AI-driven processes meet the GDPR's definition and have therefore been directly impacted by the law. Given AI's reliance on vast quantities of data, regulating AI through special privacy law is not only inevitable, but also a compelling strategy that should be carefully considered as the law explores approaches to mitigating AI's risks. Generally, the focus has been on algorithms, but as the GDPR demonstrates, data regulation can also be a tool for constraining the contexts in which AI can be used. Though the GDPR encourages privacy by design and aims to prevent any potential misuse of personal data through technology and organizational strategies, these provisions are being challenged by the new ways in which AI enables the processing of personal data. For instance, traditional data protection principles such as purpose limitation, data minimization, sensitive data handling, and automated decision restrictions are in tension with the full computing potential of AI and big data.⁵

With complex decision-making processes come extra layers of privacy considerations as data/information of individuals is processed for decision and prediction. Specific privacy laws on AI transparency would focus on understanding the workings of the AI system, including how it makes decisions and processes data. Moreover, the latest advancements in deep learning are focused on creating explainable models and allowing individuals to understand the reasons behind the decisions made by AI. This is crucial in decision-making processes that have a significant impact on society, such as health care and finance.⁶ AI transparency would build trust with customers, detect and address potential data biases, and enhance the accuracy and performance of AI systems. AI-specific privacy laws could address the need for transparency and accountability in automated decision-making. Also, there is the argument for the use of differential privacy—a privacy-enhancing technology that quantifies privacy risk to individuals when their data appear in a dataset—to publish analysis of data and trends without being

able to identify any individuals within the dataset.⁷

The GDPR provides that personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimization);⁸ however, AI systems often rely on vast amounts of data to train and improve their models, thereby raising concerns about the amount of data these AI systems collect and utilize. Data minimization includes restrictions on what data are collected, the purposes for which they can be used following collection (purpose limitations), and the amount of time firms can retain data. These rules require companies to demonstrate the necessity and proportionality of



the data processing and to prove that it is necessary to collect certain kinds of data for the purposes they seek to achieve, to state that they will only use such data for predefined purposes, or to ensure that they will only retain data for a period that is necessary and proportionate to these purposes. Typically, certain types of data classified as “sensitive” receive a heightened level of protection; for example, the collection of biometric data requires a stricter sense of necessity.⁹ For AI systems processing large amounts of data sets, the key question would be what is adequate or proportionate, as the general approach in designing and building AI systems involves collecting and using

as much data as possible, without thinking about ways they could achieve the same purposes with less data. The answer would be case-specific, and all relevant data minimization techniques for AI should be fully considered during the design phase. AI-specific privacy laws could emphasize principles such as data minimization and purpose limitation to ensure that only necessary data are collected and used for specific, legitimate purposes.

According to the president's Executive Order, it is important to ensure that AI is developed and used in a way that advances equality and civil rights. Discrimination or disadvantage should not be perpetuated using AI, but rather AI should be utilized to improve people's lives. However, AI systems can inherit biases or algorithmic fairness present in training data, which can lead to discriminatory outcomes. The Blueprint for an AI Bill of Rights¹⁰ recognizes the need for algorithmic discrimination protections to guide the use and deployment of AI systems. Specialized privacy laws could be implemented to address bias in AI systems, which could incorporate bias mitigation strategies and promote risk management measures during and after the processing of data.

MACHINE LEARNING AND THE RIGHT TO EXPLANATION

The right to explanation refers to the concept that a ML model and its output can be explained in a way that “makes sense” to a human being at an acceptable level. Certain classes of algorithms, including more traditional ML algorithms, tend to be more readily explainable while being potentially less performant. Others, such as deep learning systems, remain much harder to explain. Improving the ability to explain AI systems remains an area of active research. In its 2016 report¹¹ and guidelines from 2020, the Federal Trade Commission leaves no doubt that the use of AI must be transparent, include explanations of algorithmic decision-making to consumers, and ensure that decisions are fair and empirically sound.¹² Providing data subjects with an explanation is important as individuals have the right to be informed of how their data

are being processed, particularly when there is the existence of solely automated decision-making that produces legal or similarly significant effects. This means that individuals need to be provided with a meaningful explanation of the logic behind the AI system, as well as the possible consequences of the processing. Organizations that deploy AI technology must have detailed documentation in place to explain how and why their data are being processed. Furthermore, the data embedded in machine-learning models must be explicitly included when considering consumers' rights to delete, know, and correct their data. As AI systems make decisions that impact individuals, there is a need for privacy laws that grant individuals the right to understand and challenge decisions made by algorithms.

Additionally, AI relies on processing massive amounts of data to produce useful insights, which reinforces the importance of rules governing cross-border data transfers. AI heavily depends on other data-intensive cross-border activities that are subject to digital trade regulations, such as cloud computing services and data collection from IoT (Internet of Things) devices. Limiting cross-border data transfers as obtainable in existing privacy laws could slow down the development of AI by restricting access to training data and essential commercial services. However, the lack of a sufficient regulatory framework raises concerns about the rapid growth of AI, including the weaponization of AI, misinformation, surveillance, bias, and intellectual property protection. These risks highlight the need for privacy laws specific to AI that can provide clarity on how cross-border data transfers, especially those involving personal data, should be handled.

PROACTIVE, TRANSPARENT AI DEVELOPMENT AND POLICY

It is important to understand the complex relationship between privacy regulations and the trustworthy use of AI. In the past year, there have been various proposals to enable the development of trustworthy AI such as the NIST Artificial Intelligence Risk Management

Framework 1.0 and the president's Executive Order. On a global scale, there is the EU AI Act passed by the European Parliament and UNESCO's recommendation on the ethics of AI,¹³ which aims to establish ethical principles and values for the development and use of AI.

The extraordinary ability of AI to analyze data and make complex evaluations increases privacy concerns. To protect user privacy in the face of AI's ability to analyze data, it is essential to proactively regulate AI technology by anticipating future developments and implementing preemptive measures. Regulatory frameworks must be dynamic and responsive to the technology's changes, demanding transparency from developers about their algorithms and data sources. Developers should create models that respect user privacy by minimizing data requirements and implementing robust data protection measures, while innovative approaches like differential privacy and federated learning should be utilized. Therefore, adopting AI-specific privacy laws is crucial to address the unique challenges posed by AI.

Chuma Akana is a Tech, Law & Security Program Fellow at the American University Washington College of Law and completed his LL.M. in Intellectual Property and Technology Law. His research is focused on privacy, AI, and emerging technologies. Previously, he worked as a foreign-trained attorney and advised on global privacy compliance..

ENDNOTES

1. The White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, BRIEFING ROOM (Oct. 2023), <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. NISTAC REPORT TO THE PRESIDENT ON A CYBERSECURITY MOONSHOT (Nov. 2018), <https://www.cisa.gov/sites/>

[default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf](https://www.nist.gov/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf).

3. *Trustworthy and Responsible AI*, NIST, <https://www.nist.gov/trustworthy-and-responsible-ai>.

4. NIST, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>.

5. Lynn Parker Dupree & Taryn Willett, *Seeking Synergy Between AI and Privacy Regulations*, REUTERS (Nov. 17, 2023), <https://www.reuters.com/legal/legalindustry/seeking-synergy-between-ai-privacy-regulations-2023-11-17>.

6. Dineshkumar Muthu, *The Advancements of AI in Complex Decision Making*, MEDIUM (Feb. 1, 2023), <https://medium.com/@dineshdk2904/the-advancements-of-ai-in-complex-decision-making-c0bb2a5a59e6>.

7. Press Release, NIST, NIST Offers Draft Guidance on Evaluating a Privacy Protection Technique for the AI Era (Dec. 11, 2023), <https://www.nist.gov/news-events/news/2023/12/nist-offers-draft-guidance-evaluating-privacy-protection-technique-ai-era>.

8. Regulation (EU) 2016/679, art. 5(1)(c), 2016 O.J. (L 119) (General Data Protection Regulation).

9. *Data Minimization as a Tool for AI Accountability*, AI NOW (Apr. 11, 2023), <https://ainowinstitute.org/spotlight/data-minimization>.

10. THE WHITE HOUSE, OFF. OF SCI. & TECH. POL'Y, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE (Oct. 2022), <https://www.whitehouse.gov/ostp/ai-bill-of-rights>.

11. FTC REPORT, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (Jan. 2016), <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>.

12. Andrew Smith, *Using Artificial Intelligence and Algorithms*, FED. TRADE COMM'N: BUS. BLOG (Apr. 8, 2020), <https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms>.

13. UNESCO, RECOMMENDATION ON THE ETHICS OF ARTIFICIAL INTELLIGENCE (2022), <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>.



Generative AI Litigation A One-Year Check-In

By Luke Rushing and Samuel Lowry



As generative artificial intelligence (Gen AI) closes out its first year in the mainstream, any moderately apprised attorney is aware that recent developments in this technology will likely spur new types of litigation; the question is, how? These are still early days; there are likely to be significant developments still to come, so the categories of cases are only partially crystalized. But throwing caution to wind, there are so far five main legal theories pursued in cases revolving around Gen AI: privacy, copyright, trademark, right of publicity (and facial recognition), and tort cases. Despite the differentiation, a helpful rubric for analyzing cases from all five categories is to consider whether the harm alleged is focused on the AI *input*, the *output*, or both. Typically, input-focused claims revolve around training data, not user input, and often allege impropriety in how such data were gathered or that they were accessed in violation of intellectual property rights. Output-focused cases often allege that AI outputs violate copyrights and trademarks, or produce content that is otherwise tortious.

Before diving further into the individual categories, some common features jump out. One unifying feature across the cases is the positions of the parties: In all of the major cases filed so far, the defendant has been a company involved in Gen AI. Another nearly unifying feature is California as the forum of choice, although federal courts in Delaware and Georgia also have seen cases filed. In fact, nearly all the major cases so far have been filed in the same federal district, the Northern District of California. California state law—especially California’s Unfair Competition Law, codified at Business and Professions Code § 17200, which has been pleaded in over half the cases examined for this article—is also highly prominent, but Illinois state law has been pleaded multiple times and Delaware and Georgia state law have each been pleaded once.

GEN AI IN PRIVACY CASES

Two cases in this category have been filed thus far, both by anonymous plaintiffs against tech giants.¹ In each case, the anonymous plaintiff was represented by the same law firm, which helps explain

why both cases (one now voluntarily dismissed and the other anticipating a motion to dismiss the amended complaint) were filed in the Northern District of California and alleged violations of California’s Unfair Competition Law.

These cases are largely input-focused; the predominant claim in each is that the plaintiffs had economic and privacy rights in data that were scraped by OpenAI and Google, respectively. Google’s motion to dismiss made a wide-reaching counterargument: that the plaintiffs had failed to allege Article III standing because (1) they had not identified specific private data that had been violated and (2) they did not allege the personal information whose value was negatively impacted. Unfortunately, no court has yet weighed these theories. Google’s motion to dismiss provoked an amendment to the complaint from the anonymous plaintiffs; Google has informed the court of its intent to dismiss the amended complaint as well.²

GEN AI AND COPYRIGHT CASES

As of this writing, four major cases have been filed in this category:³ one by photographers whose work was trained on by Stability AI,⁴ one by coders whose work was trained on by Github,⁵ and two related cases by authors⁶ whose work was trained on by OpenAI.⁷ This category of claim often includes elements of input-based damages and output-based damages. For example, in all four cases, the plaintiffs alleged that a model had been trained on their copyrighted works, which were accessed without permission or proper license. However, in all four cases, the plaintiffs also alleged that outputs from the model could either resemble their works too closely or exactly reproduce their works without proper attribution (potentially violating the Digital Millennium Copyright Act).

In the *Github* case, the court noted that the input-focused claims were based mostly on privacy and property rights (but not explicitly based in copyright). The court found that the plaintiffs had not sufficiently alleged harm to these rights and consequently dismissed the input-based claims. However, the court found that the plaintiffs had adequately alleged that the model had the potential to output works

similar to the plaintiff's works. Thus, the court found that Article III standing was appropriate for the output-based claims.⁸

In the *Anderson v. Stability AI* case, on the other hand, every claim was dismissed except for the input-based claim. In that case, several plaintiffs sued over the use of their photographs as training data for the Stability Diffusion Model. The court found that the complaint was largely deficient and dismissed all but one claim. Specific to copyright, the court found that only one plaintiff had actually alleged a registered copyright in a work that was accessed by defendants without license. Only that claim was permitted to proceed. With regards to the output-related claims, the court dismissed with leave to amend after finding that the plaintiffs had unintentionally handicapped themselves by admitting that “none of the Stable Diffusion output images provided in response to a particular Text Prompt is likely to be a close match for any specific image in the training data.”⁹ This admission helps explain why the output-based claim failed in this case but succeeded in the prior case, *Doe 1 v. Github*. In *Github*, rather than admitting that outputs would not resemble the work at issue, the “Plaintiffs argue[d] that, ‘[g]iven the number of times users may use Copilot, it is a virtual certainty [that] any particular plaintiff’s code will be displayed either with copyright notices removed or in violation of Plaintiffs’ open-source licenses for profit.’”¹⁰ A clear lesson emerges here: Plaintiffs seeking to recover for output-based claims would do well to include specific, credible allegations that pieces of their works will be included in model outputs.

Both cases regarding authors, *Tremblay* and *Silverman*, have pending motions to dismiss. Coupled with the leave to amend granted in both the *Git Hub* and *Stability AI* cases, further developments will shed significant additional light on the viability of copyright-focused claims.

GEN AI AND TRADEMARK CASES

Getty Images v. Stability AI contains allegations of both copyright and trademark infringement, and I have chosen here to break out the trademark claims for a closer examination of the subject. Getty Images owns and licenses approximately

12 million images across the web. Their trademark is ubiquitous on internet images, so much so that images produced by Stability's model have often incorporated variants on the mark. Under Getty's theory, Stability infringes on Getty's mark when its models reproduce their trademark. Furthermore, because images produced by Stability are often lower quality than typical photographs (e.g., the distorted human faces and unresolved details that are hallmarks of generated images), Getty argues that their trademark is diluted when it is wrongfully associated with generated images.¹¹ Stability AI initially moved to dismiss the complaint on procedural and technical grounds before the parties agreed to conduct jurisdictional discovery. The case is stayed while that discovery is still ongoing.¹²

RIGHT OF PUBLICITY AND FACIAL RECOGNITION

This category of cases revolves around the use of facial data in image-generating (or image-modifying) software. Neither of these cases necessarily involves AI; in each instance, the AI component could simply have been any technology. Nonetheless, cases involving AI only tangentially will likely represent a significant amount of AI case law, so they still merit examination. In *Prisma Labs*, the defendant corporation owned and operated an app that allowed users to upload photos that would be converted into artistic images. Plaintiffs alleged that the software also stored those facial data without informing its users so that the data could be used to train Prisma's neural network. These allegations were brought almost entirely under Illinois state law, which is particularly plaintiff-friendly for biometric law, and did not allege any damages resulting from the Gen AI output. That case has been ordered by the court into arbitration.¹³

Similarly, in *Young v. NeoContext*, the defendant corporation operated an app that altered users' photos. But in this instance, the app also offered a premium service that advertised a model that could swap users' faces with those of celebrities. One of the celebrities promoted was reality star Kyland Young, who alleged that he never consented to the use

of his likeness and had not received compensation despite the defendant's profits. Young sued for one claim of California's right of publicity law. The defendants moved to dismiss the sole claim, but the court denied the motion. The most relevant holding for the AI industry was that replacing Young's face—while leaving his body and using AI to realistically merge the user's face into Young's body—was not transformative enough *at the motion to dismiss stage* to act as an affirmative defense.¹⁴ Purveyors of generated images should take note: If the purpose of transforming a photo still involves retaining an element that is protectable by a third party, that third party may be able to claim damages.

GEN AI AND TORT DAMAGES

Finally, *Walters v. OpenAI* raises the question of whether AI can produce content that is defamatory. A journalist investigating a legal case asked ChatGPT for information regarding the case; ChatGPT responded that Mark Walters was accused of embezzlement. In reality, Mr. Walters was accused of no such thing and was not related to the complaint being investigated.¹⁵ Walters brought a state law claim for libel in Georgia state court; the case was removed to federal court and then remanded back to state court, where it was subject to a motion to dismiss from OpenAI.¹⁶ OpenAI argued that the journalist who encountered the falsehood did not take it to be accurate and that the plaintiff could not prove actual malice from the output of a statistical model. The state court recently denied the motion to dismiss but without further analysis of the arguments at issue.¹⁷

WHAT TO WATCH IN YEAR TWO OF AI LITIGATION

Mainstream generative AI is currently in its second year and already there are multiple avenues for litigation surrounding it. Here are some of the key takeaways as we enter the second year:

It's Still Early Days

Many of the cases discussed above remain in their infancy. For the few that have had any consideration on the merits, that has only been at the motion to

dismiss stage, leaving plenty of space for additional rulings. Expect substantial new developments in all of these cases over the following year.

Federal Courts in California Are the Forum of Choice

Perhaps unsurprisingly given that the center of gravity of the tech world lies in Northern California, nearly every complaint filed has been in a California court, and almost all of those were in the Northern District of California.

Federal, California, and Illinois Law Are the Main Jurisprudence at Play

The federal copyright regime, the federal trademark regime, and the Digital Millennium Copyright Act are all regularly cited in AI cases. Furthermore, many plaintiffs have relied on California state law, especially regarding privacy and unfair competition, as well as Illinois law regarding privacy in biometric data.

Specificity Is Key

This is perhaps a practice tip applicable to all attorneys. In part due to the large number of cases decided on the motion to dismiss standard, whether plaintiffs have pleaded sufficiently specific harms is an issue courts have regularly grappled with. Successful plaintiffs have gone out of their way to allege their copyright registrations, that their works or private data were *actually* used in training data, and that outputs may resemble their data, work, or likeness. Unsuccessful plaintiffs have simply alleged in general that the entire internet was scraped for data, so their works must have been included, or any work in the training set *might* be contained in an output.

Transformation Should Be Comprehensive

Many AI services have capitalized on AI's ability to transform images and text. The ruling in *Young* implies that transformations should be comprehensive and should not intend to maintain elements of the original, or the affirmative defense of transformation may not apply.

* * *

As generative AI enters its second year, keep your eyes on this space for significant updates on the state of the law.

Luke Rushing began his career in commercial litigation focusing on entertainment law. In the years since, he has added significant civil rights and maritime work to his portfolio. As generative AI has surged in usage and in the zeitgeist, he has spoken on the subject for law firms, interviewed numerous thought leaders in the field, and served as a vice chair to the ABA's Committee on AI and Robotics.

Samuel Lowry is a legal analyst at the boutique firm of Huth Reynolds LLP and assists with issues ranging from maritime law to generative AI. He graduated from Harvard College in 2023.

ENDNOTES

1. Class Action Complaint, P.M. v. OpenAI LP, Dkt. No. 3:23-CV-03199 (N.D. Cal. June 28, 2023); Class Action Complaint, J.L. v. Google, Dkt. No. 3:23-cv-03440 (N.D. Cal. July 11, 2023).

2. Google's Motion to Dismiss Amended Complaint, *Google LLC*, Dkt. No. 3:23-cv-03440 (N.D. Cal. May 16, 2024).

3. During the writing of this article, the *New York Times* filed a copyright infringement suit against OpenAI in the Southern District of New York, yet there were no substantive updates and the answer was not due for another month at least. Complaint, N.Y. Times Co. v. Microsoft Corp., Dkt. No. 1:23-cv-11195 (S.D.N.Y. Dec. 27, 2023). The Authors Guild and others, including John Grisham and George R.R. Martin of *Game of Thrones* fame, filed a complaint against OpenAI on September 20, 2023. An amended complaint was filed on December 4, 2023, claiming copyright infringement; there have also been no substantive updates. Amended Complaint, Authors Guild v. OpenAI Inc., Dkt. No. 1:23-cv-08292 (S.D.N.Y. Dec. 5, 2023).

4. Complaint, Andersen v. Stability AI Ltd., Dkt. No. 3:23-cv-00201 (N.D. Cal. Jan. 13, 2023).

5. Class Action Complaint, DOE 1 v. GitHub, Inc., Dkt. No. 4:22-cv-06823 (N.D. Cal. Nov. 3, 2022).

6. The plaintiffs in this case include the noted comedian and television personality Sarah Silverman.

7. Class Action Complaint, Tremblay v. OpenAI, Inc., Dkt. No. 3:23-cv-03223 (N.D. Cal. June 28, 2023); Complaint, Silverman v. OpenAI, Inc., Dkt. No. 3:23-cv-03416 (N.D. Cal. July 7, 2023).

8. Order Granting in Part & Denying in Part Motions to Dismiss, *GitHub, Inc.*, Dkt. No. 3:23-cv-00201 (N.D. Cal. May 11, 2023).

9. Complaint, *Andersen*, *supra* note 4, ¶ 93.

10. Opposition/Response at 15, *GitHub, Inc.*, Dkt. No. 3:23-cv-00201 (N.D. Cal. Mar. 9, 2023), ECF No. 67 (emphasis added). While the court found that this claim did not support damages, it could support forward-looking injunctive relief.

11. Amended Complaint at 1, *Getty Images (US), Inc. v. Stability AI, Inc.*, Dkt. No. 1:23-cv-00135 (D. Del. Mar. 29, 2023).

12. Defendants' Opening Brief in Support of Their Motion to Dismiss or Transfer This Action, *Stability AI, Inc.*, Dkt. No. 1:23-cv-00135 (D. Del. May 2, 2023).

13. Complaint for Damages, *Jack Flora v. Prisma Labs Inc.*, Dkt. No. 3:23-cv-00680 (N.D. Cal. Feb. 15, 2023).

14. The court did leave room for a later finding that the face-swapping was transformative, but nonetheless seemed skeptical of the claim: "The Ninth Circuit has found that depictions that are arguably more transformative than those created with Reface do not entitle a defendant to the affirmative defense as a matter of law." Order Re Defendant's Motion to Strike & Motion to Dismiss at 14, *Kyland Young v. NeoCortex, Inc.*, Dkt. No. 2:23-cv-02496 (C.D. Cal. Sept. 5, 2023).

15. While it did not develop into a lawsuit, an additional instance of ChatGPT creating false accusations happened to professor of law Jonathan Turley. See Pranshu Verma & Will Oremus, *ChatGPT Invented a Sexual Harassment Scandal and Named a Real Law Prof as Accused*, WASH. POST (Apr. 5, 2023), <https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies>.

16. Amended Complaint, *Walters v. OpenAI, L.L.C.*, Dkt. No. 1:23-CV-03122 (N.D. Ga. Sept. 8, 2023).

17. Motion to Dismiss, *Walters*, Dkt. No. 1:23-CV-03122 (N.D. Ga. Oct. 13, 2023).



Using ChatGPT in Law School

By Harsh Mahajan

Today, we stand on the precipice of a new era, where the burgeoning landscape of artificial intelligence (AI) promises to reshape the fabric of legal scholarship and practice. This transformation echoes a striking historical parallel: the emergence of the automobile. Just as early cars initially met with skepticism and even fear, while they revolutionized transportation, AI technologies are bound to drive a similar paradigm shift in the legal world.

My own journey as a law student has been deeply influenced by my background in software engineering. In today's AI tools, I see not just a new utility but a new way of approaching long-established legal practices. This parallels one of my key takeaways from engineering: Always master tools designed to automate tasks rather than spending long hours doing them manually.

More than a technological leap, the rise of cars, or, as they were earlier called, “the horseless carriages,” necessitated a shift in perspective and adaptation.¹ Early pioneers of cars didn't just invent new machines; they had to convince the public of their utility and safety.² Similarly, the proliferation of generative AI tools like ChatGPT calls for a reevaluation of how we approach legal writing. It isn't simply about adding a new tool to our toolbox but embracing a new, AI-powered paradigm. This doesn't diminish the importance of critical thinking and legal reasoning; it merely suggests that these essential skills can be complemented and augmented by the capabilities of AI.

Taking inspiration from my engineering background, this past fall semester, I chose an unconventional path for my two term papers: I wrote them with the assistance of ChatGPT, a generative AI tool. This wouldn't have been possible without the support of my professors. One, an engineer himself, saw it as a valuable exercise in embracing technology impacting legal practice. He encouraged us to experiment in the safe haven of law school, where “failing” wouldn't carry real-world consequences. My other professor, equally supportive, requested a disclaimer on the extent of

AI assistance used. In the following sections, I'll dive deeper into generative AI, large language models like ChatGPT, and my experience using ChatGPT for these term papers.

WHAT IS CHATGPT?

The technical details of how ChatGPT works can get too convoluted too soon. So, in simple terms, ChatGPT is a tool that functions like a highly informed virtual assistant capable of generating text-based responses. It works by using a method called “transformer” technology, which is a bit like having a really good memory for patterns in language.³ ChatGPT has been “trained” by reading a vast amount of text, helping it learn how to piece together words and phrases in a way that makes sense.⁴ It is almost like it has read an enormous library of books and can recall and reuse that information to answer questions or write text.

That said, ChatGPT has its limitations. For one, it does not truly “understand” what it is talking about; it is more like it is really good at guessing based on patterns it has seen.⁵ Also, its knowledge is frozen at the point when it was last updated, currently 2021, so it will not know about recent events or the very latest trends.⁶ While it can write about a wide range of topics, it doesn't have personal experiences or feelings, so its responses can sometimes lack a human touch. Additionally, because it learns from existing text, it can sometimes repeat biases or inaccuracies found in its training material.⁷ One of the largest pitfalls of ChatGPT is that it “hallucinates”: generating incorrect or misleading results due to insufficient training data, incorrect assumptions made by the model, or biases in the data used to train the model.⁸ We are all probably familiar with the issue of the New York lawyer who used ChatGPT to draft a legal brief for a case in federal district court, and ChatGPT ended up fabricating legal cases and citations.⁹ Such awkwardness can be avoided if every user understands the limitations of the tool they are using and utilizes the tool with those limitations in mind. To me, ChatGPT is meant to

reduce human effort, not replace human intellect or creativity.

For law students, the tool's ability to generate coherent, contextually relevant responses and learn from human feedback present an opportunity to enhance legal writing. Directing ChatGPT to generate documents by providing it with the necessary information can increase efficiency and help shave off significant periods of time that can be spent on other productive tasks. The ability to have a thesis statement drafted for you, on your direction, allows more time for editing the statement, rather than having to start from scratch.

ChatGPT, in my opinion, is about to bring about a significant shift in how legal writing can be conducted, promising increased efficiency and accuracy in these critical tasks.

CHATGPT: ANOTHER TOOL IN THE SHED

Any new technology invariably reminds me of a lecture from my second year in software engineering. My professor sketched two rectangles on the blackboard, labeling one “Input/Output” and the other “Calculations,” connecting them with arrows to illustrate the basic functions of a computer. He went on to say, “Look at this idiot! It's not smart, just fast!” His point was clear: Despite their speed, computers require human oversight to produce accurate outcomes.

MATLAB (an abbreviation of MATrix LABoratory) is a coding language by MathWorks that enables one to conduct extensive mathematical computations expeditiously.¹⁰ However, should errors arise, it is obvious that the onus is on the user to validate the correctness of the code, the algorithms applied, and the results obtained. In engineering, I was taught how to use MATLAB and how to conduct mathematical computations with it, but if the result was wrong, I was the one responsible for generating a wrong output. Likewise, I believe that with ChatGPT, the onus is on the student to ensure that the result is correct. The program, here ChatGPT, simply generates what we tell it to generate. If it does

not generate what we want, we should revise what we are telling ChatGPT.

Similarly, computer-aided design (CAD) has revolutionized 3D modeling, allowing users to not only conceptualize entire gear trains but also generate precise engineering drawings instantaneously.¹¹ This stands in stark contrast to the bespoke era when drafters toiled for hours, meticulously crafting these drawings by hand. Presently, CAD facilitates the swift creation and modification of such drawings, saving drafters valuable time.¹² In our Engineering Design class in the first year of engineering, we were taught how to use Autodesk Inventor, a type of CAD. The focus was more on how to design, visualize, and integrate parts in CAD. We were taught how to read engineering drawings, build the parts from the basis of the drawings, and make free-hand sketches of the parts. Sketches are free hand, not to scale, and primarily intended to convey the idea, while drawings are precise, follow conventions, and are to scale. So, when it came to producing the drawings of our parts, we would simply click a few buttons in Autodesk Inventor to produce the required drawings with the specified conventions.¹³ One can design complex gear trains using CAD, but like MATLAB, here too, the onus is on the user to design a proper, functioning gear train.

In both cases, the user is responsible and gets the credit for the work. Similarly, I see ChatGPT as a tool that can save law students hours spent crafting the perfect thesis statement. The key is to learn how to use this tool well, to create a thesis and then refine it as needed. It is like using code to get the desired outcome: You guide ChatGPT to produce the draft you want.

HOW I USED CHATGPT TO DRAFT

As someone transitioning from engineering to law, the task of writing term papers comprising over 6,000 words seemed a Herculean task. In engineering, our reports, spanning 40–60 pages, mainly consisted of diagrams, tables, and explanations of our project's components. Our research focused on existing

solutions to a problem, followed by how our project is a more efficient approach to solving the problem. Unlike in law school, our engineering classes did not require us to write term papers based on extensive academic research, a concept unfamiliar to me. Only a small subset of engineers, who engaged in research, were familiar with concepts like building a thesis statement. To me, conducting research and building a thesis statement from it, and then an entire research paper, were a novel challenge. In staying true to my engineering practice of learning how to use a tool effectively, I turned to ChatGPT to aid in drafting my term papers. In one paper, I received a B+, and in the other, which was a bit shorter, I received an A-. For both the papers, I received the grade to which the class was curved. I could have certainly done better, but for my first attempt, I was quite content. My process involved the following steps.

CONDUCTING THE RESEARCH

Recognizing that ChatGPT's knowledge base only extends to publicly available information until 2021, I relied on traditional legal research tools such as Westlaw and LexisNexis. This step ensured I was aware of the latest research and able to identify and rectify any "hallucinations" in ChatGPT's responses. This way, because I had read the research and was aware of the arguments made in each paper, I could tell when ChatGPT had hallucinated and generated a result whose argument or logic did not align with those made in the research papers.

PRIMING CHATGPT

Priming ChatGPT is akin to dressing appropriately for a specific activity. One would not wear ski gear for fly-fishing, nor waders for skiing. Similarly, setting up ChatGPT in the correct context is crucial. Priming ensures ChatGPT understands the context and user expectations better, leading to improved results.¹⁴

One may start by telling ChatGPT the ideal person for the job. For example, in the context of drafting term papers, I began by setting the context,

telling ChatGPT, "You are a legal academic adept at writing legal research papers, and you will assist me in drafting a paper on [your topic]." Envision the ideal person for your job and describe that person to ChatGPT. The more detailed the context provided, the better ChatGPT can adapt to the role. For example, detailing the target audience, the paper's tone, key takeaways, and desired reader impact sharpens ChatGPT's focus.

Next, we want to communicate to ChatGPT its role in aiding us. For example, "I will give you the outline of my term paper, and I want you to give me feedback on the outline. Tell me if the structure makes sense or if I am missing any potential discussion points. Then, we shall work on drafting the section together."

Always ensure to ask ChatGPT to repeat the task before anything. This will ensure that we are on the same page as ChatGPT. If not, we can either edit our message or have a conversation with ChatGPT and direct it in our preferred direction.

Another way to build the context for ChatGPT is to ask it a series of questions (or queries). Here, we are having a conversation with ChatGPT, and through our queries we are helping ChatGPT reach the context in which we want it to operate, quite like the Socratic Method in law schools. The Prompt Engineering Institute offers an in-depth discussion on this priming process. It calls this a "pyramid approach," which encourages small, specific questions to help ChatGPT understand the context and for you to gauge its knowledge.¹⁵

DRAFTING WITH CHATGPT

With ChatGPT properly primed, we move into the drafting stage. Here, we provide snippets from various papers and instruct ChatGPT on how to weave these into the draft, mentioning the topic of the papers, argument structure, and desired word limit. For example, "I will give you these 2-3 articles, and I'd like you to draft a section based on them, adhering to a 500-word limit and including in-line references to the articles." It is always a good practice to ask

ChatGPT to provide in-line references to the articles so we can ensure that it is not hallucinating. Another means to ensure that ChatGPT does not hallucinate is to instruct it explicitly to only rely upon the information provided and to not seek any outside information. Here, because we asked ChatGPT to provide in-line references, we can cross-check if the argument drafted by ChatGPT matches the argument made in the article that it has referenced. If the argument drafted by ChatGPT aligns with, or uses the correct facts from, the article provided, we know that it has not hallucinated. Furthermore, as we have already done our research and read the articles ourselves, we are able to catch any argument that does not align with the provided articles.

Again, we want it to repeat our ask and ensure that we are on the same page. I often provide ChatGPT with the articles in one message. I inspect the output that ChatGPT generates. At times, regenerating a few more iterations generates a better output. Other times, a few cursory edits in the draft are sufficient. There are, of course, times when ChatGPT has totally missed the point. In such cases, you want to have a chat with it to point out what you want from it.

Wait until the very end for your introduction and your conclusion sections.

You need to keep in mind that you are in control. *You are steering the car; you are in control of this horseless carriage; if it steers itself into a ditch, you are responsible.* You need to ensure that you are directing it on how you want the content drafted. The more effectively you can convey your needs to ChatGPT, the more likely the result generated will be closer to what you intended. It does take some practice to achieve your desired results.

CHATGPT FOR FINAL TOUCHES AND PROOFREADING

Once we have performed the third stage for all the sections of our paper, we can start with the introduction and conclusion sections. Here, we

will provide ChatGPT with the existing draft of our paper and instruct it to draft the introduction and conclusion sections.

Ensure ChatGPT is aware of your expectations for the sections. For example, “Ensure the introduction section starts with a thesis statement and a roadmap. The goal of this section is to introduce the topic and ensure that the reader knows what to expect in the following sections.” You can also add certain aims like “Aim to engage the reader’s interest.” Such prompts may produce some superfluous language, which can be either edited or specified to be avoided. With regards to a thesis statement, you probably have a statement in mind or know what to say but are finding it hard to put pen to paper. You can ask ChatGPT to generate a thesis statement, telling it how you want the statement structured, and then edit it to your liking. However, my preferred way is to write my own thesis statement and ask ChatGPT to revise it in the context of all the sections that have been drafted so far.

Similarly, for the conclusion section, we can ask ChatGPT to summarize all the arguments made in the paper and leave the reader with closing remarks. As with every section, a word limit can be specified.

Finally, now that we have all the sections of our paper drafted, it is time to turn it into a single, cohesive document. Tell ChatGPT that we are going to give it a draft of the entire paper, and it is supposed to proofread it. We can ask it to make the paper cohesive, check the grammar, and improve the flow of the arguments. Or we can ask it to critique the paper and give us feedback on the paper. I prefer the latter as, in that case, ChatGPT does not redraft the paper, which helps retain footnotes.

WIDER APPLICATIONS FOR AI IN THE LEGAL PROFESSION

The ABA Model Rules state that lawyers must remain current with technological advancements and their implications.¹⁶ Artificial Intelligence is poised to transform our practice fundamentally. I personally believe that if we train ourselves to be adept at effectively using

these new tools, we can become a lot more efficient in the service that we provide to our clients. We need to ensure that we are aware of the limitations of the tools that we use. For example, sharing confidential information with ChatGPT is not wise as it stores information and learns from it. Keeping the limitations in mind is a key step in using these tools effectively. In this context, ChatGPT might well be likened to the first horseless carriage of the legal profession, signaling a significant shift in our profession. I personally feel that we are yet to see the Model T equivalent of generative AI. Playing around with these tools now would prevent potential pitfalls in the future, such as sanctions for misuse in practice due to unfamiliarity.

Law schools should attempt to integrate AI tools like Harvey.ai, LexisNexis AI, and Google’s Bard into their curriculum to prepare students for modern practice. While the LSAT ensures students can read and analyze logically, writing skills vary and are often influenced by one’s undergraduate education. Here, AI can aid in drafting legal documents, but the onus remains on law students to critically evaluate and apply their research, e.g., case law and law reviews, accurately within their work, ensuring their use of technology enhances rather than undermines the drafting of their legal arguments.

P.S. If you are wondering, then, yes, this article was drafted with the help of ChatGPT, but, naturally, a great deal of editing and revision were done outside ChatGPT. Law students must, of course, follow the rules of their law school and individual law professors surrounding the use of AI and ChatGPT.

Harsh Mahajan is a law student at Rutgers Law School in Newark, New Jersey, and a clinical research assistant at Rutgers Law School Intellectual Property Law Clinic. He holds a degree in Software Engineering from McMaster University, Canada, and previously worked in supply chain management.

ENDNOTES

1. Alexander Winton, *Get a Horse*, SAT. EVENING POST (Feb. 8, 1930).

2. Louis Anslow, *Forget Self-Driving Car Anxiety: In the Early Days Human Drivers Were the Fear*, MEDIUM (Nov. 3, 2016) (<https://medium.com/timeline/forget-self-driving-car-anxiety-in-the-early-days-human-drivers-were-the-fear-55a770262c10>).

3. See Amanda Hetler, *ChatGPT*, TECHTARGET, <https://www.techtarget.com/whatis/definition/ChatGPT> (last visited Jan. 14, 2024).

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

8. See *AI Hallucinations*, GOOGLE CLOUD, <https://cloud.google.com/discover/what-are-ai-hallucinations#:~:text=AI%20hallucinations%20are%20incorrect%20or,used%20to%20train%20the%20model>. (last visited Feb. 3, 2024).

9. Benjamin Weiser & Nate Schweber, *The ChatGPT Lawyer Explains Himself*, N.Y. TIMES (June 8, 2023), <https://www.nytimes.com/2023/06/08/nyregion/lawyer-chatgpt-sanctions.html>.

10. See *MATLAB: The Language of Technical Computing*, MATHWORKS https://www.mathworks.com/help/matlab/index.html?s_tid=hc_panel (last visited Jan. 14, 2024).

11. See Indeed Editorial Team, *What Is a Draftsman? And How to Become One in 3 Steps*, INDEED (Nov. 11, 2023), <https://sg.indeed.com/career-advice/finding-a-job/what-is-a-draftsman>.

12. Tesla Outsourcing Serv., *The Journey of CAD Services: From Drafting Tables to Digital Transformation*, LINKEDIN (Sept. 27, 2023), <https://www.linkedin.com/pulse/journey-cad-services-from-drafting-tables-digital>.

13. *To Generate a 2-D Drawing*, AUTODESK <https://help.autodesk.com/view/INVENTOR/2022/ENU/?guid=GUID-A8329377-18E0-4C79-A475-017CC0066FA1> (last visited Feb. 3, 2024).

14. Sunil Ramlochan, *Unlocking AI with Priming: Enhancing Context and Conversation in LLMs Like ChatGPT*, PROMPT ENG’G INST. (May 11, 2023), <https://promptengineering.org/unlocking-ai-with-priming-enhancing-context-and-conversation-in-llms-like-chatgpt>.

15. *Id.*

16. MODEL RULES OF PRO. CONDUCT r. 1.1 (AM. BAR ASS’N 1983).

Excellence in
data privacy
mediation.



Abe Melamed,
Mediator | Arbitrator |
Special Master

EXCLUSIVELY AT
SIGNATURE
RESOLUTION

SIGNATURERESOLUTION.COM

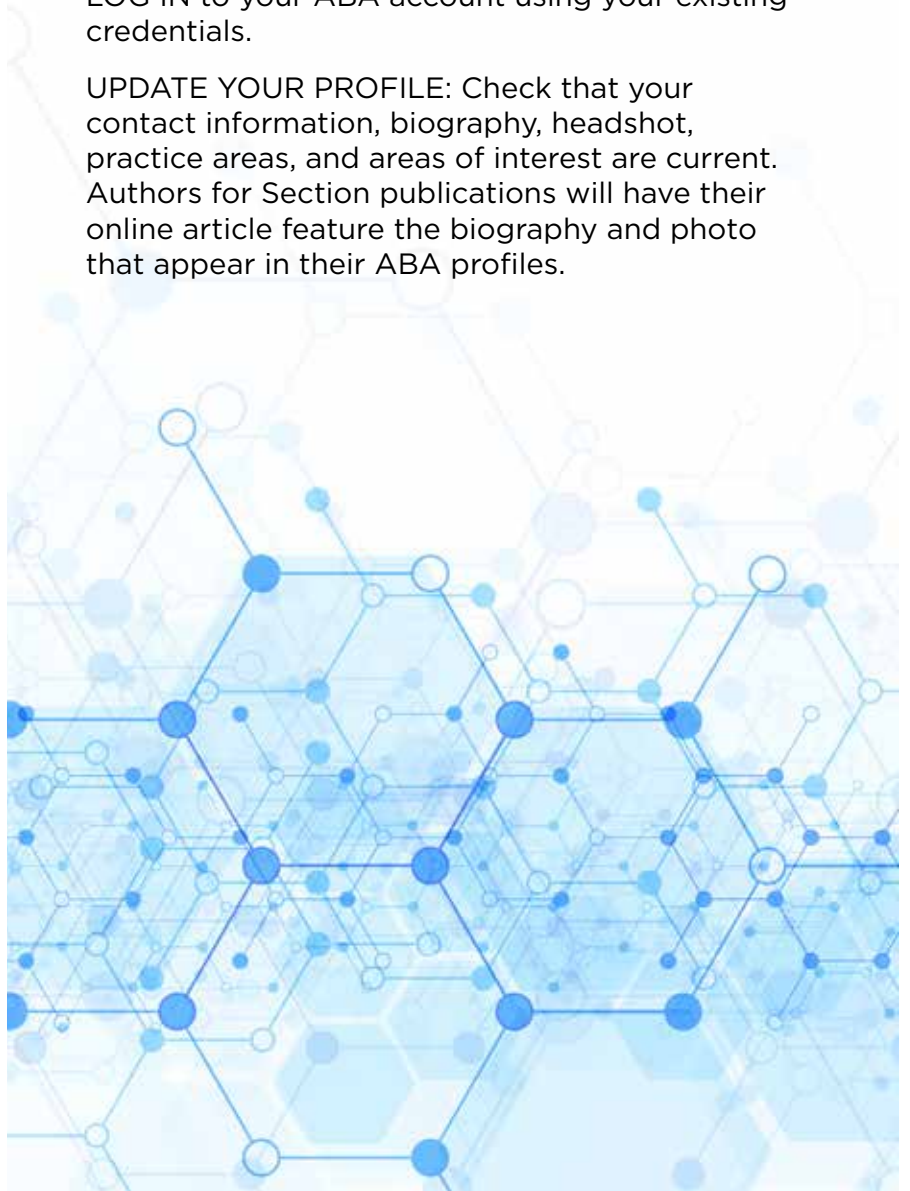
EXCITING CHANGES ARE COMING SOON TO THE ABA SCIENCE & TECHNOLOGY LAW SECTION WEBSITE!

- Streamlined Navigation
- Enhanced Search
- Most Recent Content

To get the most out of the coming web experience, if you are a Section member:

LOG IN to your ABA account using your existing credentials.

UPDATE YOUR PROFILE: Check that your contact information, biography, headshot, practice areas, and areas of interest are current. Authors for Section publications will have their online article feature the biography and photo that appear in their ABA profiles.



ABA SCIENCE & TECHNOLOGY LAW SECTION NOMINEES FOR 2024–2025 SECTION OFFICER, COUNCIL, AND SECTION DELEGATE POSITIONS

The Nominating Committee is pleased to announce the following slate of nominees for 2024–2025 Officer, Council, and Section Delegate positions in the Science & Technology Law Section. The Section membership will vote on the slate of candidates during the Section's Annual Business Meeting, which immediately follows the Council Meeting on August 2, 2024, during the 2024 ABA Annual Meeting.

SECTION CHAIR

Joan R. M. Bullock is the owner of Reformed Law Prof SM, a consulting firm with the mission of empowering legal professionals with the critical skills and tools necessary for building a



successful and sustainable 21st-century legal practice. Bullock is a Michigan lawyer and CPA who has practiced before the United States Tax Court and provided business advisory services to law firms and various organizations. She has more than 30 years of experience in the legal academy as a professor of law and more than a decade of decanal experience spanning three law schools. Bullock currently serves as chair-elect of the ABA Science & Technology Law Section. She is a fellow of the American Bar Foundation, a past chair and delegate to the ABA House of Delegates for the ABA Law Practice Division, and a former member of the Council for Racial and Ethnic Diversity in the Educational Pipeline. She is the author of *How to Achieve Success After the Bar: A Step-by-Step Action Plan* and a chapter contributor to *The Best Lawyer You Can Be: A Guide to Physical, Mental, Emotional, and Spiritual Wellness*, both published by the ABA Law Practice Division. Bullock holds a JD from the University of Toledo College of Law, an MBA from the University of Michigan Ross School of Business, and a BA degree from Michigan State University.

SECTION CHAIR-ELECT

Lois D. Mermelstein is of counsel at Garg Law Firm and also operates her own law office. She currently focuses her practice on patent prosecution, particularly for



software, semiconductors, artificial intelligence (AI), and other computer related technologies. Mermelstein also has patent litigation

experience, and prior to law school, she worked as a software and firmware engineer and team leader. Mermelstein also writes, speaks, and puts on CLE programs involving AI and other technology-related legal subjects. Mermelstein currently serves as the ABA Science & Technology Law Section's Vice Chair and is a senior editor of the *SciTech Lawyer*. She is also a past editor-in-chief of the magazine. She serves on the ABA's Standing Committee on Technology and IT, co-chairs a subcommittee focusing on AI and robotics for the Business Law Section and is Business Law's liaison to SciTech. She also chaired Business Law's Technology Committee. Mermelstein holds a BS in electrical engineering from the University of Toronto, an MS in electrical engineering from the University of Southern California, and a JD from Washington & Lee University School of Law. She is admitted to practice in Virginia, Texas, and before the USPTO.

SECTION VICE CHAIR

Matthew Henson is a founding partner of Henson Klein, where he focuses on a wide range of issues affecting corporations, including governance, intellectual property and technology licensing, and mergers and acquisitions. Henson currently serves as the secretary of the ABA SciTech Section. His experience includes representing all sides of the privately held, emerging company: founders, investors, and employees. Prior to forming the Allerton Law Group, he served as special assistant and senior advisor to Senator Bill Bradley during Senator Bradley's campaign for the presidency, and as his "traveling chief-of-staff." He has written multiple law- and business-related articles in legal and business publications, and his political analysis has appeared on the *New York Times* Op-Ed



page. Previously, Henson worked at the Boston law firm of Hill & Barlow, P.C. He graduated from Harvard Law School in 1991 with a JD *cum laude*, and from Princeton University in 1991 with an A.B. *cum laude* from its Wilson School of Public and International Affairs. At Princeton, He was a starter at forward for Princeton's Ivy League champion basketball team and was twice named a District II Academic All-American. In 1990, he played in the then-most-watched men's college basketball game in the history of ESPN (Princeton vs. Arkansas, NCAA First Round), a record that lasted for 16 years. He was recently featured in an ESPN 30-for-30 Short entitled "The Billion Dollar Game," about the Princeton-Georgetown game the previous season.

SECRETARY

Christopher A. Suarez, CIPP/US, is a partner at Steptoe LLP in Washington, D.C. Trained in electrical engineering and computer science at the Massachusetts Institute of Technology,



Chris is both a litigator and counselor whose practice focuses on emerging technologies, particularly at the intersection of artificial intelligence and the Internet of Things. His litigation experience spans patent, copyright, and trade secret litigation, and he has represented both plaintiffs and defendants at every level of the U.S. Court system, including the Supreme Court, Federal Circuit, and U.S. District Courts. As a counselor, Suarez provides advice on AI governance and policies, IP portfolio management and policies, IP licensing, and privacy. Suarez is currently serving as the Budget Officer of the ABA SciTech Section and has served on various roles and committees. He has been a co-editor of two recent SciTech books: *The Internet of Things: Legal Issues, Policy, and Practical Strategies* (2019), and the forthcoming *Artificial Intelligence: Legal Issues, Policy, and Practical Strategies* (2024). Suarez advocates for diversity and pro bono in the legal profession. He is a member of both Steptoe's Diversity and Inclusion Committee and is active in

the Leadership Council for Legal Diversity. Suarez obtained his J.D. from Yale Law School.

BUDGET OFFICER

Paul Lanois is a director at the European law firm Fieldfisher, based in the Silicon Valley, where he advises clients on data protection, privacy, and cybersecurity mat-



ters. Lanois is also an adjunct faculty at UC College of the Law, San Francisco (formerly known as UC Hastings), where he teaches privacy compliance. He is currently a member of the CIPP/US Exam Development Board at the International Association of Privacy Professionals (IAPP). Lanois has previously worked on technology transactions at large international law firms London, UK, France, and Luxembourg, was an associate professor at the University of Cergy-Pontoise Law School in France, and was vice president and senior legal counsel at a leading international bank, Credit Suisse, at its headquarters in Switzerland as well as its Hong Kong office. Lanois is also a member of the Executive Committee of the California Lawyers Association's Privacy Law Section. Paul was selected by *The Recorder* as a winner of the 2022 California Legal Awards in the category of "Lawyers on the Fast Track (under 40)." He was named in the Global Data Review "40 under 40" (2021) and in the "Cybersecurity & Data Privacy Trailblazers" by the *National Law Journal* (2016).

SECTION DELEGATE

Eric Y. Drogin is a two-term past chair of the ABA SciTech Section and a Sustaining Life Fellow of the American Bar Foundation. He serves as an instructor for the Harvard Law School Trial Advocacy Workshop and as an adjunct professor of Law and Mental Health for the University of New



Hampshire Franklin Pierce School of Law. Drogin is currently the chair of the ABA Senior Lawyers Division Center for Excellence in Elder Law and Dementia and a commissioner of the ABA Commission on Law and Aging. He was previously a co-chair of the National Conference of Lawyers and Scientists and a commissioner of the ABA Commission on Mental and Physical Disability Law. Drogin received his JD degree from the Villanova University School of Law. Currently holding faculty appointments with Harvard Medical School, the Harvard Mass General Brigham Forensic Psychiatry Fellowship Program, and the Brigham and Women's Hospital Harvard Medical School Psychiatry Residency Training Program, Drogin is a fellow of the American Psychological Association, a fellow of the American Academy of Forensic Psychology, and a Diplomate and past president of the American Board of Forensic Psychology. He is the affiliated lead of Psycholegal Studies for the Psychiatry, Law, and Society Program at Brigham and Women's Hospital. Drogin received his PhD in Clinical Psychology from Hahnemann University.

COUNCIL

Michael G. Gruden, a counsel at Crowell & Moring LLP's Washington, D.C. office, is a former Pentagon information technology acquisition branch chief and a leading cybersecurity lawyer who helps government contractors navigate privacy, cybersecurity, and contract compliance requirements. Drawing from his experience at the U.S. Department of Defense and U.S. Department of Homeland Security, Gruden represents some of the nation's largest defense contractors, cloud service providers, and tech companies. Gruden is a Certified Information Privacy Professional with a U.S. government concentration. He is also a registered practitioner under the Cybersecurity Maturity Model Certification framework. Gruden serves as co-chair of the ABA SciTech Section's Homeland Security Committee as well as the



Coalition for Government Procurement's Cybersecurity Committee. Gruden's legal practice covers a wide range of counseling and litigation engagements at the intersection of government contracts and cybersecurity. Gruden has served as a cybersecurity subject-matter expert for leading False Claims Act proceedings and investigations. His privacy and cybersecurity practice includes cybersecurity compliance reviews, risk assessments, data breaches, incident response, regulatory investigations and cyber diligence for corporate transactions. He also helps clients develop incident preparedness strategies and table-top exercises to assist companies in mitigating risks presented by data breach incidents.

COUNCIL

Tamra T. Moore is an attorney with more than 15 years of private and public sector litigation and regulatory experience, which she leverages to counsel clients navigating the gray areas associated with the intersection of technology and policy. Her private sector experience includes her current position as in-house counsel at a Fortune 500 global financial services company, where she advises the chief data officer and others on legal and regulatory compliance for the development and use of artificial intelligence and machine learning models in consumer-facing products and internal operations.



Moore's public sector experience includes over a decade as senior counsel in the U.S. Department of Justice's Civil Division, Federal Programs Branch where she served as lead counsel in over a dozen complex civil challenges filed against the United States seeking to overturn nationally significant federal government policies and programs. Moore previously served as a law clerk to judges on both the United States Court of Appeals for the Fourth Circuit and the United States District Court for the District of Rhode Island.

Moore's public sector experience includes over a decade as senior counsel in the U.S. Department of Justice's Civil Division, Federal Programs Branch where she served as lead counsel in over a dozen complex civil challenges filed against the United States seeking to overturn nationally significant federal government policies and programs. Moore previously served as a law clerk to judges on both the United States Court of Appeals for the Fourth Circuit and the United States District Court for the District of Rhode Island.

COUNCIL

Jaipat Singh Jain is a partner in the New York City law firm of Lazare Potter



Giacovas & Moyle LLP. Jain represents domestic and international technology and other clients in transactional mat-

ters, principally private mergers and acquisitions; private securities transactions; and choice, organization, and governance of business entities. His clients regularly also seek his counsel in matters relating to data transfer and privacy, licensing and development of technology, employment, distribution and supply, asset-based lending, commercial mortgage lending, leasing and conveyance of commercial real estate, and international trade and financing. His clients include fintech and telepathology companies, manufacturers of specialty chemicals, global conglomerates engaged in mining and manufacturing, private equity funds, among others.

Jain came to the United States as an international business executive, first as a manager and then as the country manager of the U.S. branch of one of South Asia's largest global trading companies. As a lawyer, he sees his role as helping clients create wealth and make sound business decisions. He is often the lawyer of choice for private transactions between India and the United States and resolution of business disputes. Jain is on the Board of Directors of the Association of the Bar of the City of New York, is a member of New York Attorney Grievance Committee (First Department), and is a life fellow of the American Bar Foundation. He has served as chair of ABA's India Committee, chair of Legal Practice, Ethics & Delivery of Legal Services Division, on the editorial board of the ABA/ Bloomberg Law Lawyers' *Manual on Professional Conduct*, and as vice chair of the EPrivacy and Cloud Computing Committees of the ABA SciTech Section. Jain is honorary trustee of International Mahavira Jain Mission (Siddhachalam), a nonprofit, and its former president and vice-chair. Jain is a frequent speaker at business and law conferences has chaired continuing legal education programs.

Get the SciTech Edge

MEMBERSHIP AND DIVERSITY COMMITTEE NEWS

BY JOANNE CHARLES



What really matters when we consider civic engagement is more than passive membership; a true connection to a community of practice requires active and involved association. Addressing the inter-

section of scientific practice, technological innovation and evolving regulation, the mission of the ABA Science & Technology Law Section is to provide leadership on emerging issues.

The ABA's 35 Sections offer members opportunities develop their legal skill through publications and continuing legal education programming. SciTech Committee members support programs and attend meetings to enhance their professional development. Whether the meetings are virtual or in-person, they support professional growth, providing opportunities to learn and network.

Our Section's commitment to education is most prevalent in the consistent and dynamic programming it offers members. In the past year, the section has offered members a number of ways to engage and connect. In April 2024, the Section hosted its inaugural Science & Technology Law Section Spring Meeting in Bethesda, Maryland. It joins the list of dynamic programming the Section offers including podcasts and publications from books to journals.

Committee programming and member resources are just some of the ways that the Section provides thought leadership. Our resources can focus in meaningful ways on important and timely topics especially artificial intelligence and machine learning's influence on technology as well as the practice of law. Members can rely on these resources for critical analysis and practical application. We are proud to have the SciTech Section Chair Laura

Possessky and many other SciTech Section leaders as members of the ABA's Task Force on the Law and Artificial Intelligence.

Despite recent challenges to principles on diversity, equity and inclusion, this Section's commitment to DEI remains firm. Diversity in the legal profession promotes the public's perception of an equal and fair judicial system and encourages thoughtful legal strategies which ultimately results in new and innovative ideas. The ABA's Diversity, Equity, and Inclusion Center's Affirmative Action Path Forward Series is a great resource.

Members get the most out of membership when they make their voices heard. For members who are seeking get more involved, there are subcommittees that can provide more focus to your practice needs, including Privacy, Security and Emerging Technologies, Life Sciences, and Law Student Engagement just to name a few. SciTech also connects experienced practitioners and new-to-practice attorneys for mentoring and networking opportunities.

Ultimately, the Section seeks to promote sound policy and public understanding on issues that impact the careers of Section members and the ABA members at large. We invite you to learn more about how you can get the most out of your membership by visiting https://www.americanbar.org/groups/science_technology/membership.

***Joanne Charles** is chair of the MAD Committee and associate general counsel at Gilead Sciences. Her work focuses on AI, privacy, and data ethics. Prior to joining Gilead, Joanne was senior corporate counsel in Microsoft's Corporate, External and Legal Affairs Department.*

Future SciTech Leaders

LAW STUDENT ENGAGEMENT COMMITTEE NEWS

BY DAVID HUSBAND AND CAYLAN FAZIO



The Law Student Engagement Committee (LSEC) has kept busy providing students an opportunity to engage with practicing lawyers in developing areas of law, such as generative Artificial Intelligence. Recently, LSEC hosted a well-attended and popular Fireside Chat with the leaders of SciTech's AI and Robotics Committee. The discussion was wide-ranging, from the question of how AI could enable the human conquest of space, to how AI might enable enhanced productivity both

in law school and practice. Below, LSEC member Caylan Fazio reflects on how AI is impacting her studies and asks wide-ranging questions about its possible effects on society and the legal profession. We continue to encourage law students to join our Fireside Chats, which will have included Homeland Security by publication, with Privacy still to come.

David Husband
—Co-Chair of LSEC

AI AND THE LAW

I remember the headlines from about a year ago: ChatGPT-4 had passed the bar exam. It was the Spring of my 1L year, and I had given little thought to AI beyond a few specific interests in technology and privacy regulations. Within the past year, I found myself discussing generative AI tools, and how they might be relevant to case readings and research projects in law school. While finding it beneficial to academic pursuits, students and professors are also questioning the limitations of this technology. How much should we permit it to be used as a tool? How do we maintain academic integrity while using generative AI tools?

Alongside students, the legal community has grappled with similar issues over the past year, truly running the gamut of both legal and ethical questions. We are only in the initial stages of AI's involvement in the practice of law, yet it is already clear that the opportunities for

innovation expand to all edges of the legal profession, from research database products to understanding the rules of professional conduct.

This past year has already demonstrated some limits and cautionary tales for generative AI. The need for a deeper understanding is crucial for its mindful and responsible involvement. Law students, as the next generation of legal professionals, have the opportunity to embrace these questions and contribute to discussions in the ABA's SciTech Committees.

Students' involvement in AI is crucial, and the ABA is a perfect platform for students to explore their interests. Rapidly changing technology only adds to the skills expected from a new lawyer, including skills in appropriately querying AI sources and awareness of its limitations and ethical use. Beyond these technical skills, students should think deeply about how they are involving AI to safeguard justice. Will AI allow for greater access to justice? Or will inequity in this emerging technology further gaps in access to justice? This generation of law students will be crucial in shaping the framework for responsible use.

The recent fireside chat with co-chairs Matt Henson, George A. Long, and Luke Rushing of the AI and Robotics Committee highlighted the novel challenges AI poses to law and society in general. Discussions like this encourage students to explore fast-growing legal areas and build connections with professionals. We encourage students to attend the fireside chats as opportunities to learn more about the committee's work and expertise in that field. Stay tuned for more information on upcoming events.

David Husband is co-chair of the Law Student Engagement Committee in ABA's SciTech Section and works as a senior counsel for the Board of Governors of the Federal Reserve System.

Caylan Fazio is a second-year law student at Cleveland State University College of Law. Her legal interests include space law, data privacy, and tax law.

SCIENCE & TECHNOLOGY LAW SECTION

American Bar Association
321 North Clark Street
Chicago, Illinois 60654-7598
PC54580002003

Nonprofit
Organization
U.S. Postage
PAID
American Bar
Association

**ALSO FROM THE
SCIENCE &
TECHNOLOGY LAW
SECTION**

- » *SciTech e-Merging News* quarterly electronic newsletter
- » *Jurimetrics Journal* quarterly electronic law review
- » Free hot-topic committees and listservs
- » Networking opportunities
- » CLEs, webinars, and podcasts
- » Books to enhance your practice
- » Members-only discounts
- » And much more



CALENDAR

AUGUST 1-2, 2024
ABA Annual Meeting
 Chicago, IL
ambar.org/annual

OCTOBER 14-15, 2024
**Artificial Intelligence and Robotics
 National Institute 2024**
 Santa Clara University School of Law
ambar.org/scitech

**ARTIFICIAL INTELLIGENCE (AI)
 AND ROBOTICS**

NATIONAL INSTITUTE 2024

SAVE THE DATE
October 14-15, 2024

SANTA CLARA UNIVERSITY SCHOOL OF LAW



CONNECTWITH#SCITECH

ambar.org/SciTech

www.facebook.com/ABASciTech

twitter.com/ABASciTech

www.linkedin.com/company/aba-scitech