HansonBridgett

Artificial Intelligence:

Legal Challenges and Emerging Solutions

RESOURCE MATERIALS

TUESDAY, MARCH 19, 2024

LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com

TUESDAY, SEPTEMBER 6, 2022

PERSPECTIVE

The humans win round one

By Robert A. McFarlane
and Rosanna W. Gan

Artificial intelligence (AI) has long been a subject of fascination and has populated science fiction stories for decades. Isaac Asimov imagined intelligent robots in the 1940s and fashioned his immutable "Three Laws of Robotics" to prevent them from harming their human creators. Astronaut Dave Bowman fought for his survival in a confrontation with an intelligent computer named HAL in the climactic scenes of 2001: A Space Odyssey. An episode of Star Trek the Next Generation called "The Measure of a Man," depicted a judicial hearing to determine whether the sentient android Lieutenant Commander Data was an autonomous being with legal rights or nothing more than a complex machine that could be downloaded and disassembled in the name of research. And, more recently, an AI robot named Ava prevailed over her human creator in the 2014 movie Ex Machina.

AI now exists outside the confines of futuristic stories and is embedded in a multitude of commonly used technologies. AI curates what we see on social media, encourages our online shopping with disturbingly accurate suggestions for things for us to buy, and interacts with us through personal assistants like Siri and Alexa. AI tools are being used to diagnose cancer and other life-threatening diseases. AI is controlling self-driving cars and autonomous vehicles. Indeed, AI has become so ubiquitous that we interact with it every day without giving it much thought at all.

Predictably, the widespread use of AI has led to numerous complex legal issues. Some of the issues currently being considered include: whether datasets supporting AI tools used to screen job applicants perpetuate discrimination based on race and gender; whether the use of proprietary AI systems in generating criminal sentencing recommendations violate a defendant's due process rights; and whether the extensive use of AI circumvents important privacy protections. In August, the Federal Circuit Court of Appeals, which has exclusive jurisdiction over patent appeals, weighed in on an issue of particular interest to intellectual property attorneys – whether an AI machine can be named as the inventor on a U.S. patent. *Thaler v. Vidal*, 43 F.4th 1207, 2022 WL 3130863 (Fed. Cir. 2022).

Steven Thaler developed the AI system "Device for the Autonomous Bootstrapping of Unified Science," or "DABUS," that he contends generates patentable inventions. *Id.* at *1. Thaler subsequently filed applications seeking patent protection for two of DABUS' purported inventions. The first application, titled "Devices and Methods for Attracting Enhanced Attention," disclosed a beacon or light source that was calibrated to a specific frequency corresponding to certain human brainwave activity. The second application, titled "Food Container," disclosed a design for a container with a complex, interlocking surface structure that was based on a fractal geometry pattern.

Thaler maintained that the inventions were "generated by artificial intelligence," that he "did not contribute to the conception of either of these inventions[,] and that any person having skill in the art could have taken DABUS' output and reduced the ideas in the applications to practice." *Id.* If DABUS was a person, such evidence of conception would have established that he or she was the inventor. *See, e.g., C.R. Bard, Inc. v. M3 Sys. Inc.*, 157 F.3d 1340, 1352 (Fed. Cir. 1998) ("The 'inventor,' in patent law, is the person or persons who conceived the patented invention.").

In determining whether DABUS could properly be named as an inventor, the Federal Circuit found that it did not need to engage in "an abstract inquiry into the nature of inventions or the rights, if any, of AI systems." *Thaler*, 2022 WL 3130863 at *1. Instead, the court determined that the analysis "begins and ends with the plain meaning of the [statutory] text." *Id.* at *4.

"The Patent Act expressly provides that inventors are "individuals." *Id.* at *2 (citing 35 U.S.C. §100(f)). Supreme Court precedent establishes that "'individual' ordinarily means a human being," and dictionaries confirm that "individual" is commonly understood as a "single human being." *Id.* at *3 (citations omitted). Moreover, the Federal Circuit's own precedent holds that "inventors must be natural persons and cannot be corporations or sovereigns." *Id.* at *4 (citations omitted). Thus, the court concluded that inventors must be "natural persons," i.e., human beings, thereby categorically excluding AI systems from being named as inventors on United States Patents. *Id.* at *5.

Thaler does not address patent protection for "inventions made by human beings with the assistance of AI," *id.* at *4 (emphasis in original), which is perhaps a question of greater immediate interest

Robert A. McFarlane *is a partner at Hanson Bridgett LLP and co-chairs the firm's Intellectual Property Practice. He can be reached at rmcfarlane@hansonbridgett.com.* **Rosanna W. Gan** *is a senior counsel at Hanson Bridgett LLP and focuses on IP litigation and appeals. She can be reached at rgan@hansonbridgett.com.*

given the current state of AI development. However, the holding that AI by itself cannot be named as an inventor will have increasing significance as ever more sophisticated AI is used in the creation of novel and valuable inventions.

Patent rights originate with the inventor, see 35 U.S.C. §101 (providing that "whoever invents" any patentable subject matter, "may obtain a patent therefor"), and a patent that does not name the correct inventor is invalid. *See id.; In re Verhoef*, 888 F.3d 1362, 1365 (Fed. Cir. 2018) (interpreting former 35 U.S.C. 102(f)). Under *Thaler*, if a patent application names an AI as the inventor, the patent cannot issue. If, on the other hand, an application names the person who used or controlled the AI when, in fact, the AI independently generated the patentable idea, will that patent be invalid for naming the wrong "inventor"? This potential Catch-22 could leave inventions created by AI outside the protections of the patent system.

Thaler's holding raises a host of issues for innovators using AI. Companies and their attorneys will need to evaluate whether AI-created inventions can be protected as trade secrets. They will need to determine the scope of AI-generated subject matter when deciding whether to seek patent protection and will need to insure any patent claims they file have human, rather than AI, inventors. Finally, companies relying on AI will need to work with their attorneys to develop case-specific IP strategies that encourage investment in ground-breaking inventions developed using AI that, under *Thaler*, cannot be protected by the traditional step of seeking patent protection. Barring Supreme Court or Congressional action that permits an AI to be designated as an inventor, these strategies may be increasingly important as AI becomes even more valuable as a research and development tool.

In-House Counsel

Circuit Decision on AI Complicates Inventor Strategies

By Robert A. McFarlane and Rosanna W. Gan

Sept. 14, 2022

The Federal Circuit recently found as a matter of statutory interpretation that AI systems are not eligible to be inventors under US patent statutes. Hanson Bridgett attorneys write that patentees need to be cautious in their intellectual property strategies regarding AI-generated subject matter until Congress amends or the Supreme Court interprets the patent statutes with respect to AI.

The Federal Circuit recently held as a matter of statutory interpretation that an artificial intelligence system cannot be named as an inventor on a US patent application.

This holding, which effectively excludes AI systems from the category of “individuals” eligible to be named as inventors, may complicate the intellectual property strategies of innovators who use advanced AI for research and development. Here’s what happened and why it matters.

The Federal Circuit was asked to determine whether an AI system called DABUS could be named as the inventor on two separate patent applications. The first disclosed a light source that was calibrated with a specific frequency corresponding to, among other characteristics, certain human brainwave activity.

The second disclosed a design for a beverage container that, rather than being smooth like ordinary containers, had a complex surface structure based on fractal geometry.

The circumstances surrounding the creation of these two inventions was highly unusual. Steven Thaler, the named plaintiff, and creator of DABUS asserted that DABUS generated both of the inventions without any contribution from Thaler and, further, that any person having skill in the art could have taken DABUS’ output and reduced the ideas to practice.

Interestingly, Thaler’s assertion that DABUS independently “conceived” of these inventions, which is traditionally considered to be the mental part of the inventive act, was not disputed in the record.

“Conception” is ordinarily the touchstone of inventorship. Consequently, if DABUS had been a natural person, there would have been little dispute that he or she should be named as the inventor.

The Federal Circuit, however, found as a matter of statutory interpretation that an AI system is simply not eligible to be an inventor under the US patent statutes.

Patent Rights Originate With Inventor

The unequivocal holding that AI cannot be named as an inventor on a US patent application may become more important as increasingly sophisticated AI systems are used to generate novel and valuable inventions.

One of the foundations of patent law is that patent rights originate with the inventor. This well-known principle is reflected in the contracts that commonly require employees to assign inventions to their employers.

Thaler’s holding to preclude AI systems from being listed as patent inventors may create a category of orphan inventions. If an AI independently “conceives” of a patentable invention, just as DABUS purportedly did, no patent can issue with the AI named as the inventor.

At the same time, if a patent substitutes the name of a natural person for the AI as the inventor, when the person did not contribute to the conception of the invention, that patent would be subject to invalidation for naming the wrong inventor. This conundrum may leave inventions independently “conceived” by AI ineligible for patent protection.

Limited Impact for Now

For now, *Thaler’s* impact may be limited. The Federal Circuit stated that its decision does not address patent protection for inventions made with the assistance of AI, which is likely the far more common scenario at the present time.

If a researcher uses AI as a tool, the use can be analogized to using a computer to conduct complex calculations, data analysis, or simulations in which case the researcher directing or using the AI is likely to be the appropriate inventor.

As AI becomes more sophisticated, however, more research may resemble the facts considered in *Thaler*, in that the AI machine may actually “conceive” of potentially patentable inventions.

Congress or the Supreme Court could fill the *Thaler*-sized hole in inventorship eligibility by amending or interpreting the patent statutes to recognize that a natural person controlling, programming, or providing input to an AI is considered the “inventor” for the purposes of applying for patent protection on inventions potentially “conceived” by AI.

Unless and until that occurs, however, patentees may need to be cautious in their IP strategies regarding AI-generated subject matter.

For inventions that cannot readily be reverse engineered, AI-created advances may be subject to protection as trade secrets. For inventions that can be easily copied, such as DABUS' fractal beverage container design, patent protection may remain the only viable form of IP protection.

In those circumstances, inventors and their patent attorneys will need to identify any AI-generated subject matter. They should document the ways in which that subject matter could be considered as being produced under the direction or input of the natural person to be named as inventor—which could render the AI nothing more than a research tool.

Finally, they need to work together to draft claims that cover ideas conceived by the human inventor.

Companies may also want to consider strategies based on a patchwork of patent and trade secret protections to encourage investment in groundbreaking inventions developed using AI that, under *Thaler*, cannot be protected by the traditional step of seeking patent protection.

Unless the Supreme Court or Congress step in to allow an AI to be designated as an inventor or the natural person controlling, programming, or providing input to the AI to be the inventor of any AI "conceived" invention, such strategies may become increasingly important as the capabilities of AI grow.

This article does not necessarily reflect the opinion of The Bureau of National Affairs, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

Robert A. McFarlane is a registered patent attorney and partner at Hanson Bridgett. He co-chairs the firm's intellectual property practice, has been litigating patent cases in jurisdictions across the US for 25 years, and teaches patent law as an adjunct professor at the University of California, Hastings College of the Law. He can be reached at rmcfarlane@hansonbridgett.com.

Rosanna W. Gan is a senior counsel at Hanson Bridgett is an experienced patent litigator who focuses on patent and IP litigation and on complex appellate matters. She can be reached a rgan@hansonbridgett.com.

Volume 6, No. 2 | March–April 2023

RAIL The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Volume 6, No. 2 | March–April 2023

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2023 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com
or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Federal Circuit Decision Casts Doubt on Availability of Patent Protection for AI-Generated Inventions

Robert A. McFarlane and Rosanna W. Gan*

In this article, the authors discuss a recent federal circuit court decision holding that an artificial intelligence system cannot be named as an inventor on a U.S. patent.

The U.S. Court of Appeals for the Federal Circuit, in *Thaler v. Vidal*,[1] has ruled that an artificial intelligence (AI) system cannot be named as an inventor on a U.S. patent. The court's decision stems from a straightforward interpretation of the relevant patent statutes. However, the ruling may make it difficult to obtain intellectual property protection for inventions generated by advanced AI systems.

Ordinarily, the person who conceives of an invention is permitted to file for patent protection and initially owns any resulting patent.

Thaler, however, creates a category of otherwise patentable inventions—those "conceived" independently by advanced AI systems—that now arguably have no qualified inventor and, therefore, may not be eligible for patenting.

Inventorship Springs from Conception

U.S. patent laws have "operated on the premise that rights in an invention belong to the inventor" since enactment of the earliest patent statutes in 1790.[2] "Although much in intellectual property law has changed in the [230] years since the first Patent Act, the basic idea that inventors have the right to patent their inventions has not,"[3] and the current patent statutes provide that "[w]hoever invents or discovers any new and useful process,

Robotics, Artificial Intelligence & Law / March–April 2023, Vol. 6, No. 2, pp. 103–110.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

machine, manufacture of composition of matter . . . may obtain a patent therefor."[4] Simply put, the ownership of a patent "springs from invention."[5]

The "inventor" in patent law is the person or, in the case of joint inventors, the persons who "conceived" of the invention,[6] and conception is commonly referred to as the "touchstone of inventorship."[7] Conception is "the formation in the mind of the inventor, of a definite and permanent idea of the complete and operative invention, as it is [t]hereafter to be applied in practice."[8] Conception is completed when "only ordinary skill would be necessary to reduce invention to practice, without extensive research or experimentation."[9]

"It is elementary that inventorship and ownership are separate issues,"[10] and inventors are free to assign their rights in an invention to third parties.[11] Consequently, "inventorship is a question of who actually invented the subject matter claimed in a patent" while ownership "is a question of who owns legal title to [that] subject matter . . . , patents having the attributes of personal property."[12] "Thus, although others may acquire an interest in an invention, any such interest—as a general rule—must trace back to the inventor."[13]

Case law has limited inventors to "natural persons."[14] As a result, corporations ordinarily obtain patent rights to the inventions of their employees through formal assignments based on or required by employment contracts.[15]

If inventorship is limited to natural persons, what happens if an invention is "conceived" independently and entirely by an AI system and there is no natural person who was involved in the conception? Faced with this question, the Federal Circuit adhered to the case law holding that only natural persons can be named as inventors and categorically held that AI systems cannot be named inventors on U.S. patents.[16]

While *Thaler* expressly avoided "metaphysical matters" regarding "the nature of invention or the rights, if any, of AI systems,"[17] its impact on AI-generated subject matter is significant. A patent that does not name the correct inventor may be rendered invalid.[18] Indeed, the U.S. Patent and Trademark Office (USPTO) concluded that both of the patent applications in *Thaler* were incomplete because they lacked a valid inventor.[19]

Consequently, under *Thaler*, otherwise patentable subject matter that is independently "conceived" by an AI system may be deemed to have no cognizable inventor and that no valid patent may be issued to claim it.

Thaler Presented Inventions Created Solely by the AI System DABUS

Plaintiff-Appellant Stephen Thaler developed an AI system called "Device for the Autonomous Bootstrapping of Unified Science," referred to as "DABUS," that he contends generates patentable inventions.[20] Thaler filed applications seeking patent protection for two of DABUS's purported creations.[21]

The first application, called "Devices and Methods for Attracting Enhanced Attention," disclosed a light source that pulses at a frequency and fractal dimension that is allegedly highly noticeable to humans, which allows it to serve an effective emergency beacon because it can quickly draw a person's attention even in chaotic environments that have multiple random and distracting light sources.[22] The second application, called "Food Container," disclosed a design for a "fractal container" that can be used for storing food and beverages.[23] Rather than being smooth like ordinary containers, the surface of the claimed container had a complex surface structure based on fractal geometry.[24] The application explained that this novel construction provided several advantages over conventional packaging, including the ability to interlock containers such as soda bottles rather than having to tie them together with separate packaging elements such as a six-pack ring.[25]

Thaler asserted that the two claimed inventions were generated by DABUS, that Thaler did not contribute to their conception, and that any person having skill in the relevant arts could have taken DABUS's output and reduced the ideas set forth in the applications to practice.[26] Moreover, the patent office did not challenge these assertions and Thaler's representations were taken as undisputed facts for purposes of the opinion.[27] Based on this record, DABUS's conception of the claimed subject matter would have established its inventorship without controversy if DABUS was a natural person. But as DABUS is a machine, that was not the case.

The Parties' Arguments for and Against DABUS as a Named Inventor

While recognizing that prior cases held that inventors must be natural persons, Thaler argued that AI was "fundamentally different" from corporations and state sovereigns and that recognizing

DABUS as an inventor was critical to serving the purposes behind the patent statutes.[28]

In a nutshell, Thaler argued that the patent laws were written before the possibility of AI inventors and that the statutes should be construed to include an AI as a possible inventor in order to serve the purpose of the Patent Act to encourage inventions, their disclosure, and their commercialization.[29]

Furthermore, Thaler argued, preventing AI from being listed as an inventor removes the incentive to disclose otherwise patentable inventions generated by AI. Instead, such ideas would have to be maintained as trade secrets, and the public would lose the benefit of patent disclosure. This would frustrate the constitutional and statutory purposes of patent law to promote the progress of science and the useful arts.[30]

In response, the USPTO presented a much simpler argument based primarily on the plain meaning of the statutory language.[31]

Primarily, the USPTO argued that term "inventor" is defined in the statute to mean an "individual," and that "individual" is referenced elsewhere in the statute with the pronouns "himself or herself."[32]

These terms indicate an inventor must be a natural person, which comports with case law to the same effect.[33]

Because the plain language is unambiguous, there is no reason to look to the purpose of the statute, or to policy.[34]

And, finally, it is Congress, not the courts, who should address this issue.[35]

The Federal Circuit Unequivocally Held That AI Cannot Be Named as an Inventor

The Federal Circuit sided unequivocally with the USPTO, finding that its task "begins—and ends—with consideration of the applicable definition of the relevant statute," and that the "statute unambiguously and directly answers the question" at hand.[36] Looking to the statutory language, the Patent Act provides that inventors are "individuals."[37] Case law has construed "individual" to mean a human being,[38] dictionaries confirm this understanding,[39] and the Federal Circuit's own case law supports the construction of an "individual as a natural person."[40] Finally, the Patent Act also uses personal pronouns—himself and herself—to refer to an "individual."[41]

The court also summarily dismissed Thaler's policy arguments relating to the constitutional purpose of the patent statutes to encourage public disclosure and technological advancement, finding that they were speculative and lacked basis in the language of the Patent Act.[42] Moreover, the court found that, in light of the unambiguous statutory text, it could not "elevate vague invocations of statutory purpose" over the plain statutory language.[43]

Thaler and a Brave New World of AI-Generated Inventions

Thaler did not address the patentability of inventions made by human beings with the assistance of AI,[44] and such inventions are likely patentable to the same extent as any other inventions that are conceived with the assistance of advanced computer modeling or data manipulation. Given the present state of AI technology, the situation considered in *Thaler*, where the AI indisputably "conceived" of the patentable subject matter, may be an outlier for the time being. However, with quickly advancing AI technology, it is only a matter of time before AI-generated inventions become more commonplace.

Thaler correctly argued that the constitutional purpose of the patent law is to further the advancement science and the useful arts. By granting exclusive rights to the inventor for a limited amount of time, the patent system encourages investment in research and development by rewarding the fruits of such efforts and allowing patentees to exclude others from making, using, selling, offering to sell, or importing the patented invention during the term of the patent.[45] In today's economy, patentable subject matter is commonly generated by employees who are required to assign their inventions to their corporate employer. Thus, while the patent right originates with the human inventors, the right to enforce the patent is assigned to the employer along with the economic benefit of the patent monopoly. In this fashion, corporations are encouraged to invest billions of dollars in research and development and to employ the researchers who generate technological breakthroughs.

On its face, there is arguably no reason to treat the use of AI-generated subject matter differently than human-generated inventions under the current incentive system. Just as with their current investments in research and development efforts that do not use

AI, corporations and individual inventors can be further encouraged to invest in developing inventions with advanced AI systems by the knowledge that the fruits of those efforts would be subject to patent protection.

Indeed, Thaler attempted to effectuate that outcome using current forms and procedures. Thaler provided a statement that he executed on behalf of DABUS to satisfy the statutory requirement that inventors submit a sworn oath or declaration establishing that they are the true and correct inventor.[46] He also filed what he called a "Statement on Inventorship," explaining that DABUS was "a particular type of connectionist artificial intelligence" called a "Creativity Machine," along with a document purporting to assign himself all of DABUS's rights as an inventor.[47] However, because DABUS was found to be ineligible to be named as an inventor, this attempted solution failed.

Conclusion

Absent a Supreme Court ruling reversing *Thaler*, Congress may want to consider amending the patent statute so that, in the case of inventions "conceived" by AI systems, the inventor is deemed to be the human operating, controlling, and/or providing input to the AI system. That would clear up any ambiguity regarding inventorship of patentable subject matter generated by AI systems and encourage the on-going investment in developing and using advanced AI systems.

Notes

* Robert A. McFarlane, a registered patent attorney and partner at Hanson Bridget LLP, co-chairs the firm's intellectual property practice. He also teaches patent law as an adjunct professor at the University of California, Hastings College of the Law. Rosanna W. Gan, a senior counsel at the firm, is an experienced patent litigator who focuses on patent and intellectual property litigation and on complex appellate matters. The authors may be contacted at rmcfarlane@hansonbridgett.com and rgan@hansonbridgett.com, respectively.

[1] Thaler v. Vidal, 43 F.4th 1207, 2022 WL 3130863 (Fed. Cir. 2022). The pagination of the Federal Reporter has not been finalized, so the Westlaw pagination is used herein.

[2] Bd. of Trustees of Leland Stanford Junior Univ. v. Roche Molecular Sys., Inc., 563 U.S. 776, 780, 131 S. Ct. 2188 (2011); *see also id.* at 785-86 (cit-

ing Gayler v. Wilder, 51 U.S. 477, 493, 13 L.Ed. 504 (1850) ("the discoverer of a new and useful improvement is vested by law with an inchoate right to its exclusive use, which he may perfect and make absolute by proceeding in the manner which the law requires"); Solomons v. United States, 137 U.S. 342, 346, 11 S. Ct. 88, 34 L.Ed. 667 (1890) ("whatever invention [an inventor] may thus conceive and perfect is his individual property")).

[3] Bd. of Trustees of Leland Stanford Junior Univ., 563 U.S. at 785.

[4] *Id.* (citing 35 U.S.C. § 101).

[5] Teets v. Chromalloy Gas Turbine Corp., 83 F.3d 403, 407 (Fed. Cir. 1996); *see also* Beech Aircraft Corp. v. EDO Corp., 990 F.2d 1237, 1248 (Fed. Cir. 1993) (an invention presumptively belongs to its creator).

[6] *See* C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340, 1353 (Fed. Cir. 1998).

[7] *See, e.g.*, Ethicon, Inc. v. U.S. Surgical Corp., 135 F.3d 1456, 1460 (Fed. Cir. 1998).

[8] Hybritech Inc. v. Monoclonal Antibodies, Inc., 802 F.2d 1367, 1376 (Fed. Cir. 1986) (citations omitted); *see also* Burroughs Wellcome Co. v. Barr Labs, Inc., 40 F.3d 1223, 1227-28 (Fed. Cir. 1994) (referring to conception as "the completion of the mental part of invention").

[9] Hybritech Inc., 802 F.2d at 1376 (citation omitted); *see also* Burroughs Wellcome Co., 40 F.3d at 1228 ("An idea is definite and permanent when the inventor has a specific, settled idea, a particular solution to the problem at hand, not just a general goal or research plan he hopes to pursue.").

[10] Beech Aircraft Corp., 990 F.2d at 1248.

[11] *See* Bd. of Trustees of Leland Stanford Junior Univ., 563 U.S. at 786 (citing United States v. Dubilier Condenser Corp., 289 U.S. 178, 187, 53 S. Ct. 554 ("A patent is property and title to it can pass only by assignment").

[12] Beech Aircraft Corp., 990 F.2d at 1248.

[13] Bd. of Trustees of Leland Stanford Junior Univ., 563 U.S. at 786.

[14] *See, e.g.*, Univ. of Utah v. Max-Planck-Gesellschaft zur Forderung der Wissenschaften E.V., 734 F.3d 1315, 1323 (Fed. Cir. 2013) ("[I]nventors must be natural persons and cannot be corporations or sovereigns.").

[15] *See* Bd. of Trustees of Leland Stanford Junior Univ., 563 U.S. at 786 ("The respective rights and obligations of employer and employee, touching an invention conceived by the latter, spring from the contract of employment") (internal quotations omitted).

[16] Thaler, 43 F.4th 1207, 2022 WL 3130863 at *4.

[17] *Id.* at *1.

[18] *See* C.R. Bard, Inc., 157 F.3d at 1353 ("To invalidate a patent based on incorrect inventorship it must be shown not only that the inventorship was incorrect, but that correction is unavailable under [35 U.S.C. § 256]."); *see also* 35 U.S.C. § 256(b) ("The error of omitting inventors or naming persons who are not inventors shall not invalidate the patent in which such error occurred if it can be corrected as provided in this section.").

19. Thaler, 43 F.4th 1207, 2022 WL 3130863 at *2.

20. *Id.* at *1.

21. *Id.* (citing U.S. Patent Application Serial Nos. 16/524,350 (teaching a Neural Flame) and 16/524,532 (teaching a Fractal Container).

22. Thaler v. Vidal, Case No. 2021-2347 (Fed. Cir.), Corrected Opening Brief for Plaintiff-Appellant Stephen Thaler (Docket No. 26, filed Dec. 9, 2021) (Thaler's Opening Brief), App'x 34 and 38.

23. *Id.* at App'x 76 and 78.

24. *Id.* at App'x 78.

25. *Id.*

26. Thaler, 43 F.4th 1207, 2022 WL 3130863 at *1.

27. *Id.* at *1, fn. 2.

28. *See* Thaler's Opening Brief at 24, 30-31.

29. *See id.* at 23 (citing Application of Sarkar, 588 F.2d 1330, 1332 (CCPA 1978)).

30. *Id.* at 30.

31. *See* Thaler v. Vidal, Case No. 2021-2347 (Fed. Cir.), Corrected Combined Brief and Supplemental Appendix for the Defendants-Appellees—Andrew Hirshfeld and the United States Patent and Trademark Office (Docket No. 39, filed Feb. 10, 2022).

32. *Id.* at 19-20 (citations omitted).

33. *Id.* at 25-26 (citations omitted).

34. *Id.* at 18-19.

35. *Id.* at 30-31.

36. *See* Thaler, 43 F.4th 1207, 2022 WL 3130863 at *1 and 5.

37. *Id.* at *2 (citing 35 U.S.C. § 100(f) and (g)).

38. *Id.* at *3 (citing Mohamad v. Palestinian Auth., 566 U.S. 449, 454 (2012)).

39. *Id.* (citing, e.g., Oxford English Dictionary (2022) (giving first definition of "individual" as "[a] single human being")).

40. *Id.* at *4 (citing Univ. of Utah, 734 F.3d at 1323 (Fed. Cir. 2013) ("[I]nventors must be natural persons and cannot be corporations or sovereigns."); Beech Aircraft Corp., 990 F.2d at 1248 ("[O]nly natural persons can be 'inventors.'")).

41. *Id.* (citing 35 U.S.C. § 115(b)(2)).

42. *Id.*

43. *Id.*

44. *Id.*

45. *See* 35 U.S.C. § 271.

46. Thaler, 43 F.4th 1207, 2022 WL 3130863 at *1.

47. *Id.*

Protecting artificial intelligence requires arsenal of intellectual property laws

By Robert A. McFarlane, Esq., Hanson Bridgett LLP

MARCH 31, 2023

Artificial Intelligence suddenly seems to be everywhere. ChatGPT is writing human-sounding sermons, news updates, and answers to law school exam questions, while Dall·E is generating images ranging from the lifelike to the surreal in response to virtually any prompt.

With much less fanfare, AI has already become ubiquitous in myriad ways. AI curates social media feeds and generates purchasing suggestions to fill internet shopping carts. AI saves lives by identifying potential pharmaceutical compounds and by quickly and accurately interpreting medical scans and images. And AI is learning to drive.

> *Innovators working with AI are seeking to protect the valuable intellectual property at the heart of their business models. However, the current IP landscape complicates efforts to protect AI-related subject matter.*

AI is even making inroads to the tradition-bound and technology-resistant legal profession. Lawyers are using AI to streamline eDiscovery reviews and, more experimentally for now, to create first drafts of common legal documents.

Indeed, AI feels much like the internet did in the late 1990s. Its time has arrived. It is being widely adopted. And it is transforming everything it touches in ways that are impossible to predict.

Like so many tech companies before them, innovators working with AI are seeking to protect the valuable intellectual property at the heart of their business models. However, the current IP landscape complicates efforts to protect AI-related subject matter.

One of the biggest obstacles to protecting material generated by AI can be the lack of a human creator. This issue has been explored by an AI developer named Stephen Thaler through his efforts to patent and copyright creations generated by an AI system called DABUS. Thaler filed patent applications seeking patent protection for two inventions — a food container incorporating fractal geometry and an emergency beacon that pulsed at a frequency determined by fractal dimensionality — that the DABUS AI purportedly created without human contribution.

The USPTO rejected the applications as incomplete for the simple reason that they lacked a human who could be named as the inventor. When Thaler appealed to the U.S. Court of Appeals for the Federal Circuit, the court chose to avoid weighty "metaphysical matters" regarding "the nature of invention or the rights, if any, of AI systems." *Thaler v. Vidal*, 43 F.4th 1207, 1210 (Fed. Cir. 2022).

Instead, the court treated the issue as one of straightforward statutory interpretation and ruled that the patent laws clearly limit inventorship to human beings. *Id*. Without a human inventor, DABUS' inventions were left as unpatentable orphans beyond the protection of the patent system.

Thaler has filed a writ of certiorari, but given the unambiguous statutory language and decades of case law limiting inventorship to natural persons, it seems unlikely that the Supreme Court will intervene. "U.S. Supreme Court asked to decide if AI can be a patent 'inventor,'" Reuters Legal News, March 17, 2023, https://reut.rs/40vfoao.

Thaler's efforts also exposed difficulties in protecting AI-generated output through copyright registrations. Thaler asked the United States Copyright Office to recognize DABUS as the author of a two-dimensional work of art entitled "A Recent Entrance to Paradise," a fanciful image of a railroad track disappearing into a peaceful floral setting. Once again, Thaler claimed that DABUS produced the subject matter without any creative input from a human actor. *See* https://bit.ly/3lsAwzb.

Citing long-standing precedent, the USCO ruled that copyright protection was limited to works that are the product of human authorship and denied the requested registration. *Id*. at 3. Thaler is challenging this ruling in the federal district court case *Thaler v. Perlmutter*, case number 1:22-cv-01564 (U.S. District Court for the District of Columbia).

Because Thaler asserted that the subject matter in both instances was created without human contribution, the decisions involving

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

DABUS did not determine whether subject matter created partly by an AI or by a human using AI as a tool could be protected. The USCO took up these issues when Kristina Kashtanova sought a copyright registration for a comic book that she created using the Midjourney artificial intelligence. *See* https://bit.ly/3TF9uBd. The work at issue included text written by Kashtanova and images created by Midjourney that Kashtanova had selected, coordinated and arranged into the final compilation.

The USCO determined that Kashtanova could register a copyright for the work's text and for the "selection, coordination, and arrangement of text created by the author and artwork generated by artificial intelligence." *Id*. at 12. The text was the product of human authorship and both aspects of the issued registration reflected sufficient creativity to be protected by copyright. *Id*. at 4-5. However, the registration explicitly excludes "artwork generated by artificial intelligence." *Id*.

Just as in *Thaler*, the AI-generated images lacked a human author. Moreover, Midjourney's output could not be meaningfully predicted by its users, which distinguished it from other tools used by artists in creating works that can be protected by copyright. *Id*. at 10.

The subject matter created by DABUS and Midjourney demonstrate limits on protecting AI-*generated* content through patents and copyrights. Unfortunately for AI developers, the Supreme Court's decision in *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014), also complicates gaining patent protection on the AI systems themselves.

Alice created a two-step analysis to determine whether a claimed invention is eligible for patent protection. Under the first step, the court asks whether a patent claim is directed to ineligible subject matter such as an abstract idea, law of nature, or natural phenomenon. If the answer to that question is "yes," the court must then ask whether the claimed invention adds an "inventive concept" sufficient to transform the ineligible subject matter into a patent-eligible application.

The USPTO and the courts have found a multitude of patents drawn to software-based inventions and inventions that rely on the use of algorithms are patent-ineligible. Since AI systems are broadly based on software incorporating algorithms, inventors seeking to patent AI-related advances must carefully consider *Alice* in drafting their patent claims and in deciding whether to seek patent protection at all.

Given the limitations on patenting and copyrighting AI-related subject matter, trade secret principles offer an attractive alternative. Trade secret law protects "all forms and types of financial, business, scientific, technical, economic, or engineering information" so long as the information's owner has "taken reasonable measures to keep such information secret," and "the information derives independent economic value … from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." 18 U.S.C. §1839(3).

Requirements centering on secrecy preclude trade secret protection for non-confidential outputs of AIs such as ChatGPT or Dall·E. However, trade secret law is well adapted to protect a host of AI-related material including training data, AI software code, input parameters, and AI-generated output that is intended only for internal and confidential use. And, significantly, there is no requirement that a trade secret be created by a human being, and AI-generated material is treated like any other information. *See. e.g.*, 18 U.S.C. §1839(4) (defining trade secret owner).

The current legal landscape presents a complex environment that demands a pragmatic and nuanced approach to protecting AI-related intellectual property. Copyright can protect AI software code, human compilations and arrangements of AI-generated images. Patents can be used to protect aspects of AI systems that can pass the two-step *Alice* test.

Trade secrets can be used to protect confidential features of AI systems and their outputs, so long as reasonable steps to maintain their secrecy are taken, the material remains confidential, and competitors are not able to derive the material through legitimate or independent means. Thus, companies using or generating valuable AI will need to determine the most valuable aspects of their systems and their outputs and draw from a range of IP theories to tailor their intellectual property strategies and ensure protection for their most important AI-related developments.

About the author

Robert A. McFarlane is a registered patent attorney and litigation partner at **Hanson Bridgett LLP** where he co-chairs the intellectual property practice. He teaches patent law as an adjunct professor at the University of California College of the Law, San Francisco. He is based in San Francisco and can be reached at rmcfarlane@hansonbridgett.com.

This article was first published on Reuters Legal News and Westlaw Today on March 31, 2023.

HansonBridgett

Entertainment

The WGA's Strike Rules Provide Guidance on What is Allowed and Prohibited During the Strike

June 16, 2023

On May 2, 2023, the Writers Guild of America (“WGA”) commenced a strike after failing to secure a new Minimum Basic Agreement with the Alliance of Motion Picture and Television Producers (“AMPTP”). The two parties were unable to agree on key terms, including the minimum size of writers’ rooms, residuals from streaming, and the use of artificial intelligence. Even with the Directors Guild of America (“DGA”) reaching an agreement with AMPTP, the strike has entered its second month and the two parties continue in stalemate.

Until the strike ends, the WGA has published official “*Strike Rules*” providing guidance on what activity is allowed and what activity is prohibited. The basic principle behind these rules is that WGA Members (or their agents/other representatives acting on their client’s behalf) may not (a) meet or negotiate with a struck company; or (b) provide writing services for, or sell or option literary material to, a struck company.

Key Points

- Writers may perform other work during the strike, so long as such work is unrelated to writing and does not otherwise violate the Strike Rules.
- Importantly, there are no circumstances under which a WGA Member can render writing services for a "struck company" (i.e., a company that is a signatory to the prior Basic Agreement) during the strike.

What WGA Members are prohibited from doing

- WGA Members are prohibited from providing any writing services to a struck company.
- WGA Members may not continue to write or complete writing started before the strike for a struck company, including making changes or revisions to the literary material.
- WGA Members cannot attend meetings or engage in conversations as a writer with any struck companies concerning new, pending, or future projects/writing assignments with producers.

- WGA Members may not write for any non-union writing projects or non-signatory foreign producers.

What WGA Members are allowed to do

- WGA Members may pursue any other line of business that is not otherwise prohibited by the Strike Rules.
- WGA Members may work on "spec scripts" (i.e., a script that the writer is not commissioned by a company to write).
- WGA Members may write for outlets not covered by the WGA, such as books (fiction and nonfiction), magazines, other articles, and poetry.
- While WGA Members may continue performing purely producing, directing, or acting functions (but see below under Other Considerations concerning “hyphenates”), members are encouraged to refuse to perform any work for struck companies to assist the strike effort.

What WGA Members are required to do

- WGA Members must picket and/or perform other strike support duties.
- WGA Members must inform the guild of any witnessed strikebreaking activity.

Other Considerations

- So-called “hyphenates” (such as writer-producers, writer-directors, writer-actors) may continue to perform such other services during the strike, but cannot provide any writing services, no matter how minimal.
- Writers performing services involving fictional podcasts or fully animated programs are advised to consult with the WGA before taking any action.
- Many animators are members of the International Alliance of Theatrical Stage Employees’ Animation Guild (“TAG”). Certain animation projects are covered under TAG’s Basic Agreement, while others are covered under the WGA’s Basic Agreement. TAG is not on strike. Accordingly, TAG Members can continue to meet, pitch, and develop animated shows at TAG and non-WGA companies. However, TAG is advising its members not to meet with, pitch to, or develop content for companies involving any WGA covered work.

While the strike continues, changes to the Strike Rules may occur over the next few weeks. Hanson Bridgett will continue to monitor developments as they arise.

Hanson Bridgett Summer Associate Kevin Chaey contributed to this article.

CONTACTS

Harry Rimalower
Counsel
Los Angeles, CA
(213) 395-7620
HRimalower@hansonbridgett.com

Alfonso Estrada
Partner
Los Angeles, CA
(213) 395-7633
AEstrada@hansonbridgett.com

This article is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, does not create an attorney-client relationship, and may not be relied upon as legal advice.

AI⚙BUSINESS STAY UPDATED

NLP Chatbots Language models AI Policy

AI, Copyright Law and the Requirement of Human Authorship

An opinion piece by the IP attorneys at Hanson Bridgett LLP

Kristine Craig, Robert McFarlane and Andrew Stroud

June 26, 2023

7 Min Read

The U.S. Copyright Office recently proclaimed that most forms of AI-generated content are not entitled to copyright protection. This latest directive came in an official policy titled “Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence,” which effectively excludes AI-generated works from receiving copyright protection because they lack a human author.

This categorical exclusion reaffirms the long-standing requirement of human authorship that gained national attention in 2014, when a crested macaque monkey took a selfie using wildlife photographer David Slater’s camera and sparked a debate over who owned the copyright.

Fast forward to 2023, the most talked-about topic in the legal community is about AI. Its unprecedented pace of development, combined with an array of previously unresolved legal questions, has led experts in intellectual property law to consider the implications for creators using AI and generative AI systems.

Generative AI is a type of AI model that allows users to create content such as digital artwork, text, audio, video, speeches, poems, short stories and other media using chatbots. Common, and increasingly familiar, examples include ChatGPT, Bing Chat, and Bard, as well as AI art systems such as Stable Diffusion, Midjourney, and DALL-E. Writers have used images generated by AI to create graphic novels, and others have taken to publish AI-written e-books on Amazon.

ability to prevent unlicensed or unaccredited usage of the content.

Requirement of human authorship

Copyright is a form of intellectual property that protects "original works of authorship" from the moment the work is "fixed in any tangible medium of expression" and provides those who do so with the exclusive legal right to publish, perform, or record various works of expression, including text, photographs, video and audio recordings, artwork and software code.

Copyright law also permits original authors to sell their copyright and to grant licenses so that others can publish or otherwise use or reproduce the copyrighted material. Publishing a copyrighted work (for example by posting it on the internet, copying or distributing the work) without a license from the author constitutes copyright infringement.

Authors can register their works with the U.S. Copyright Office to gain additional legal rights and benefits, which include creating a public record of the work's origin and a legal presumption ownership, and providing the named author with the right to bring a federal lawsuit for copyright infringement and recover statutory damages and attorney's fees.

Copyright cases decided in the 19th Century tended to focus exclusively on protecting "the fruits of intellectual labor" which were "founded in the creative powers of the mind." However, the Copyright Act of 1976 explicitly recognized the vital role that technology plays in fixing or capturing copyrighted works, by describing mediums of expression as sources from which the work "can be perceived, reproduced or otherwise communicated, *either directly or with the aid of a machine or device*."

Despite this statutory language, courts and the Copyright Office have continued to grapple with drawing the boundaries of copyright protection when technology is involved, refusing to grant copyright protection to a tie-dye process as well as artwork created by a computer algorithm, but granting protection to a photograph edited with Adobe Photoshop.

confident monkey named Naruto who used Slater's camera to snap a selfie.

When Wikimedia Commons sought to publish the photograph for distribution in its collection of free online images, Slater claimed ownership, which led to a lawsuit between PETA, Slate and Wikimedia. PETA claimed in the lawsuit, which has become widely known as "the Monkey Selfie Case," that the monkey Naruto was the rightful copyright owner. In a 2017 decision, U.S. District Judge William Orrick found "no indication" that the Copyright Act extended to animals and held that Naruto could not own a copyright.

The Copyright Office followed suit and declared that the monkey's photograph was not eligible for federal copyright registration and that only works created by human beings — not those created by nature, animals or even the Holy Spirit, as alleged in a 1995 copyright case — could be registered. As a result of these rulings, works lacking a human author cannot be copyrighted and, therefore, can be freely used by anyone.

The Copyright Office's guidance on protecting AI

Since the unfortunate Naruto lost his copyright battle, the Copyright Office has confirmed that works created "without any creative contribution from a human actor" cannot be registered for copyright protection.

For example, in 2018, the Copyright Office rejected an "application for a visual work that the applicant described as 'autonomously created by a computer algorithm running on a machine.'" Most recently, in February 2023, the Copyright Office found that images in a comic book called Zarya of the Dawn, which were generated by the text-to-image engine Midjourney, could not be protected by copyright. However, the office found that the author was entitled to limited copyright protection on the text, which she had written, and on the selection, coordination and arrangement of the work, which she had fashioned to incorporate the AI-generated images.

Finally, in March 2023, the Copyright Office published a statement of policy which expressly excluded AI-generated content from copyright protection, save for a few exceptions regarding works that transform AI-generated content with sufficient creative expression.

The Copyright Office clarified its process of evaluating an application for works involving AI, which involves a determination of whether the program is merely "an assisting instrument, or whether the traditional elements of authorship in the work (literary, artistic, or musical expression or elements of selection, arrangement, etc.) (are) actually conceived and executed not by man but by a machine."

The Copyright Office also stated that it will consider on a case-by-case basis whether the asserted "AI contributions are the result of 'mechanical reproduction' or instead of an author's 'own original mental conception to which (the author) gave visible form,'" depending on "how the AI tool operates and how it was used to create the final work."

Indeed, in certain non-AI applications, depending on the degree of human involvement, even a work that is generated in part by a non-human author, such as a "celestial being" as alleged by a churchgoing-author in a 2003 copyright case, can gain protection.

Thus, given the possibility that works *incorporating* non-human input may be protected in some fashion by copyright, one may wonder about the level of protection available where a user prompts an AI system with a detailed and specific set of instructions, so as to convey a particular creative vision for the output. As applied to programs such as ChatGPT or Dall-E, which utilize textual prompts, the Copyright Office takes a limited view of human contributions to generative AI.

Using ChatGPT vs. Adobe Photoshop

systems interpret prompts and generate material" and that "when an AI technology determines the expressive elements of its output, the generated material is not the product of human authorship." Therefore, prompt-based AI systems as currently configured simply do not generate copyrightable material because they, rather than the human operator, create the output.

In reaching this conclusion, the Copyright Office specifically distinguished how artists create works with assistance from other technology such as Adobe Photoshop. Users of Photoshop or other well-established tools select the visual material they wish to modify, choose which tools to use and what changes to make, and then take specific steps to control the final image such that the resulting output amounts to the artist's "own original mental conception, to which (they) gave visible form."

By contrast, even generative AI programs that require the user to input detailed prompts do not generate copyrightable material because, ultimately, it is the AI and not the human user who controls and generates the final output.

Given that the main goal of copyright protection is to reward creative expression, the difference between rewarding human creators versus those who query ChatGPT, Dall-E or similar AI programs comes down to recognizing what is and, just as importantly, what isn't creative expression.

At least for now, human creators remain the only candidates who may obtain copyright protection and the law simply does not permit the delegation of creative acts to non-human AI actors.

Read more about:

ChatGPT / Generative AI

About the Author(s)

IP attorneys at Hanson Bridgett LLP

See more from Kristine Craig, Robert McFarlane and Andrew Stroud

You May Also Like

NLP ton Creates Its 'Most Ambitious' AI Group

August 01, 2023

NLP AI Introduces 'Custom Instructions' for Personalized ChatGPT Outputs

July 21, 2023

NLP GPT Faces First-ever Web Traffic Decline: Hiccup or New Trend?

July 06, 2023

NLP force's New AI Models Could Improve Data Analysis

July 03, 2023

CALA

News & Views

Issue 47 | August 2023

technology

AI RESHAPING ASSISTED LIVING

FOSTERING A *Culture* OF TECHNOLOGICAL INTEGRATION AND ENTHUSIASM

SCALING THE TECHNOLOGY **LADDER**

ELEVATE MARKETING *through* INNOVATION

BRINGING AI INTO FOCUS

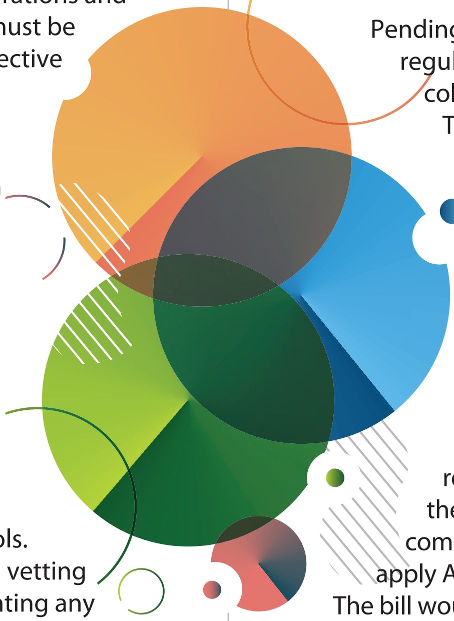
BALANCING INNOVATION WITH LEGAL AND ETHICAL RESPONSIBILITIES

By Warren Hodges, Hanson Bridgett LLP

The integration of artificial intelligence (AI) technologies has the potential to revolutionize senior care, enhance quality of life for older adults and improve operational efficiency. AI technology detects falls, captures video leading up to the fall, automates alerts to staff, and allows providers to track falls and improve care planning.

"Artificial intelligence" is, in essence, an attempt to mimic human-level intelligence in computational programs by using data and algorithms to "teach" the machine how to make decisions. AI is familiar to anyone who has interacted with voice-controlled virtual assistants like Siri or Alexa, received suggestions for certain TV shows on streaming services or news articles online, or experienced targeted advertising. The more recent "generative" AI tools are capable of more complex and increasingly independent learning as they become trained on large data sets from which they extract patterns and relationships between words and images. Generative AI appears in large language models such as ChatGPT and Bard, which hold human-like conversations based on the user's text, as well as image-generating tools like Midjourney, which can create images from written text.

As AI tools improve and proliferate, senior care organizations should approach their use with deliberation and careful attention to the legal and ethical risks involved. It is crucial to be aware of the legal considerations and regulations surrounding this emerging technology. Privacy, data security, ethical considerations and regulatory compliance are essential factors that must be carefully addressed to ensure responsible and effective AI implementation.



AI tools are effective because they are trained on massive sets of data. Where that data comes from and how it is maintained is critically important to using AI tools safely, appropriately, and in compliance with expanding governmental regulation over their use. Consequently, effective compliance begins with having at least a basic understanding of the technology's uses, limits and risks, including assurance that companies are only collecting and using data to which it has lawful access. An important first step is partnering with a reliable, trustworthy and committed technology company providing AI tools. Leaders should undertake extensive research and vetting processes before choosing a partner or implementing any technology.

It is also important to understand existing regulations governing the collection and use of the data powering AI tools. Additionally, while personal health information subject to HIPAA is exempt under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), the CCPA and CPRA strictly regulate the collection, use and dissemination of consumer data. Where providers intend to use the technology to process the personal information of employees or personal information obtained through website traffic, providers must ensure that they obtain consent, clearly communicate the uses of the technology, establish procedures to handle data requests, and develop policies governing data retention and breach notifications.

A data breach involving AI tools has the potential to be catastrophic for companies reliant upon data to train its tools. Senior care providers should look at systems that offer encryption techniques to secure sensitive resident data and restrict its use, conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in data systems, collect only the data necessary to perform the defined task, and anonymize resident information whenever possible.

Another key concern arising from the collection and use of data is the potential for bias. AI algorithms are only as unbiased as the data they are trained on and the safeguards imposed upon those training the systems and reviewing their outputs. Thus, a critical component in training AI tools is regularly reviewing tools to detect and eliminate bias. Such bias, if unmonitored, could infect critical decisions from admissions criteria to employment decisions. Leaders must collaborate with their technology providers, third-party experts, and legal counsel to continually monitor and mitigate bias caused by the use of AI technologies.

While leaders must take steps now to conform their use of emerging technologies within existing regulatory frameworks, new regulations are also on the horizon. A host of federal agencies have issued regulations or guidance on the use of AI, such as guidance from the Equal Employment Opportunity Commission on avoiding disability discrimination in the use of AI, and the White House's proposed "AI Bill of Rights."

Pending federal legislation includes proposals to regulate or ban the use of certain AI tools or collection of biometric data for machine learning. The European Union has approved its "Artificial Intelligence Act," which provides a vast regulatory framework limiting the use of AI and may serve as a framework for regulators in other parts of the world. New York City and the State of Illinois have enacted laws regulating employers' use of AI in making automated employment decisions.

California is likely to follow suit. California's Assembly Bill 331 died in committee but could reemerge in future legislative sessions. If passed, the bill would have imposed vast and onerous compliance requirements upon companies that apply AI tools in making "consequential decisions." The bill would have defined a "consequential decision" to include activities related to health care or health insurance, employment considerations, housing determinations and accreditation processes, to name just a few examples.

Companies deploying AI tools for covered purposes will be required to know what data is collected and how it is used, describe the safeguards implemented to protect against "foreseeable risks," assess potential adverse impacts on protected characteristics such as age or sex, and a host of other requirements designed to mitigate adverse impacts caused by AI tools.

AI has the potential to revolutionize the delivery of care to California's seniors. By careful planning and paying close attention to the emerging regulatory landscape governing AI and data collection, leaders can continue to improve the lives of seniors safely, ethically and compliantly. ■

Warren Hodges is counsel for Hanson Bridgett LLP. Warren specializes in employment law providing litigation, advice and counsel services for private and public employers in California. Warren has represented many senior care organizations over the last decade, as well as other health care providers. Warren is also the chair of Hanson Bridgett's AI Task Force.

Technology Artificial Intelligence AI

Latest copyright ruling should give brands pause for thought on AI creativity

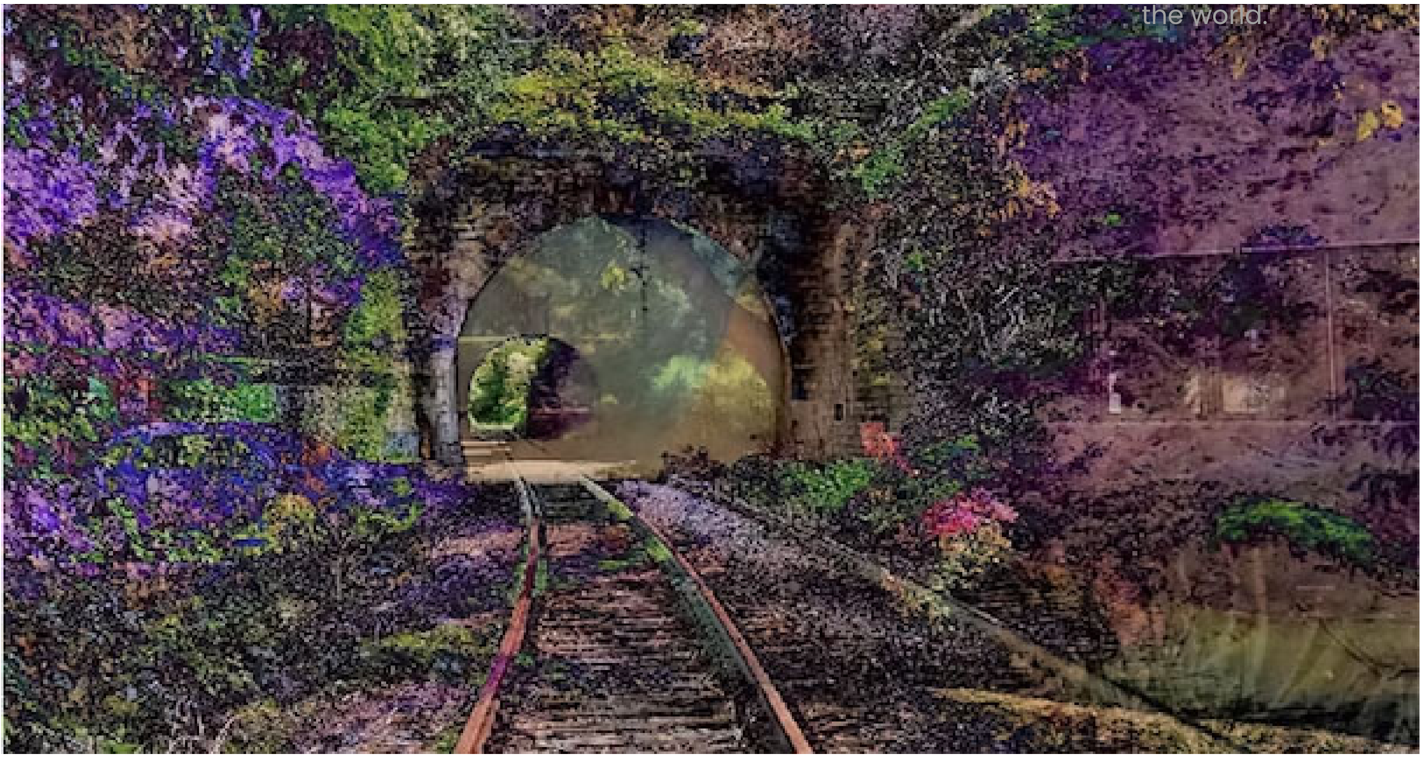
Share

By Webb Wright | NY Reporter

AUGUST 25, 2023 | 9 MIN READ

Listen to article 6 min 43 sec

A federal judge has denied copyright protection for a piece of digital artwork that was generated entirely by AI. The ruling is just the latest in a string of cases which are gradually shaping the US legal system's stance on generative AI.



“A Recent Entrance to Paradise” was supposedly created entirely by an AI model. / Stephen Thaler

The legal landscape surrounding the use of generative AI is continuing, slowly but surely, to come into focus.

Last Friday, a US district judge Beryl Howell denied inventor Stephen Thaler’s request to copyright a piece of digital artwork that had been generated "autonomously" – according to court documents – by AI. In a series of applications to the US Copyright Office beginning in 2018, Thaler claimed that the artwork in question, a trippy creation titled “A Recent Entrance to Paradise,” should be legally entitled to copyright protection due to the fact that it had been created entirely by a device of his own making, which he had dubbed the Device for the Autonomous Bootstrapping of Unified Sentience, or DABUS.

The Copyright Office rejected Thaler’s multiple applications on the grounds that the artwork had been created without human input – a prerequisite for copyright protection in the US – prompting him to sue the government agency and its director.

In her ruling, Howell determined “that the Copyright Office acted properly in denying copyright registration for a work created absent any human involvement.” She cited several copyright cases from US legal history to support her decision, including a case in text, which was claimed to be of divine origin, was ultimately eligible for copyright protection in light of the fact that it was "at least partially the product of human creativity."

On Thursday, the US Supreme Court declined to consider a challenge from Thaler against the Copyright Office's decision, according to Reuters.

"We strongly disagree with the District Court's decision," Thaler's attorney, Ryan Abbott, told The Drum on Thursday evening. "In our view, the law is clear that copyright law is intended to benefit the American public by promoting the generation and dissemination of new works, regardless of how those works are made. Denying protection for AI-generated works will be a major disincentive to the use and development of AI in the creative economy, and we plan to appeal."

Thaler's case is the latest in a series of cases that are collectively determining the character of the US legal system's stance towards generative AI, a rapidly advancing technology that many believe will have serious implications for professionals in marketing. Hollywood is also feeling the impact from the rise of the technology; one of the major concerns for protestors in the ongoing WAG and SAG-AFTRA strikes is the possible use of generative AI within the TV and film industries (to compose scripts, for example). In June, a lawsuit filed on behalf of the comedian and author Sarah Silverman, along with two other authors, claimed that the tech companies OpenAI and Meta had illegally used the plaintiffs' copyrighted material in order to train large language models.

Many creative professionals whose roles are likely to be impacted by generative AI therefore view the technology with some ambivalence. On the one hand, there's a widespread acknowledgment among this demographic that it could present new creative opportunities and eliminate a significant amount of human drudgery; on the other hand, it presents some serious legal risks, particularly when it comes to copyright and intellectual property.

A number of prominent brands, seemingly having reached the conclusion that the tial benefits of generative AI outweigh its risks, have eagerly begun to leverage the technology for marketing purposes. Many of those brands are quick to claim that

However given the fact that generative AI is still relatively new (ChatGPT was only released last November), brands haven't had many tangible legal guardrails to constrain their use of the technology. Friday's ruling against Thaler's request for copyright protection could mark a change – albeit a slight one – in the laissez-faire attitude with which marketers have until now been allowed to use generative AI.

“The district court decision, along with the prior rulings in this area, make it clear that material generated solely by an AI cannot be patented or copyrighted,” says Robert McFarlane, a patent attorney who's unassociated with the Thaler case. “However,” McFarlane adds, “that does not end the story for marketing firms and other companies who incorporate AI-generated material into their copy.”

McFarlane points to the recent case of an artist named Kristina Kashtanova who sought copyright protection for a partially AI-generated graphic novel called Zarya of the Dawn. The operative word in that last sentence is “partially”: though Kashtanova had written the text for the book and arranged its overall format herself, she had also included images that were created by the text-to-image AI model Midjourney. In its decision, issued in February, the US Copyright Office stated that “the images in the [graphic novel] that were generated by the Midjourney technology are not the product of human authorship,” and that the work as a whole was thereby only eligible for “limited” protection under copyright.

“In short, it's clear that material generated solely by AI cannot be protected by copyright,” McFarlane says, while human-made artwork which incorporates some AI-

Shyamkrishna Balganesh, a professor at Columbia Law School who specializes in copyright law, says that the federal judge's decision to deny Thaler's request for copyright protection "was fully expected in light of how prior courts have emphasized the human authorship requirement for copyright protection." He adds that this case stands out for the fact that Thaler was claiming that his AI model had been entirely responsible for the creation of the work in question, "thus denying the existence of any significant human involvement in the creative process."

Enjoy a lunchtime read

Marketing

Soiled briefs: your parody ad won't make a mark, here's the fix

Marketing

Less time at bars and pubs, more marathons: A snapshot of our 2024 leisure lives

Agencies

Ogilvy's latest partnership tests how far strategists can trust an AI focus group

This will probably be the exception to the rule, in Balganesh's view. "Most cases are unlikely to involve such expansive claims and will instead concede the existence of some human element in the creative process," he says. "In such cases, the challenge will be determining whether the AI system assisted the human creator, thereby rendering

Marketing

can
change
the world.

For more on the latest happenings in AI, web3 and other cutting-edge technologies, sign up for The Emerging Tech Briefing newsletter.

Technology Artificial Intelligence AI

Industry insights

View all

Add your own content +

Remerge

Mobile marketing in 2024: Expert insights on what to expect

Depositphotos

What photos to choose for sales campaigns in 2024: 7 trends to explore

Tagger by Sprout Social

Only 28% of women occupy c-suite roles - here are 4 ways to change that

Trending

Marketing

Soiled briefs: your parody ad won't make a mark, here's the fix

Creative

Bold & beautiful Black History Month campaigns, from Urban Outfitters, Audible & more

Marketing

Here's what's on the menu for The Drum's Focus Weeks

Close Ad

Marketina

Technology Artificial Intelligence Generative AI

What you need to know about copyright issues surrounding generative AI

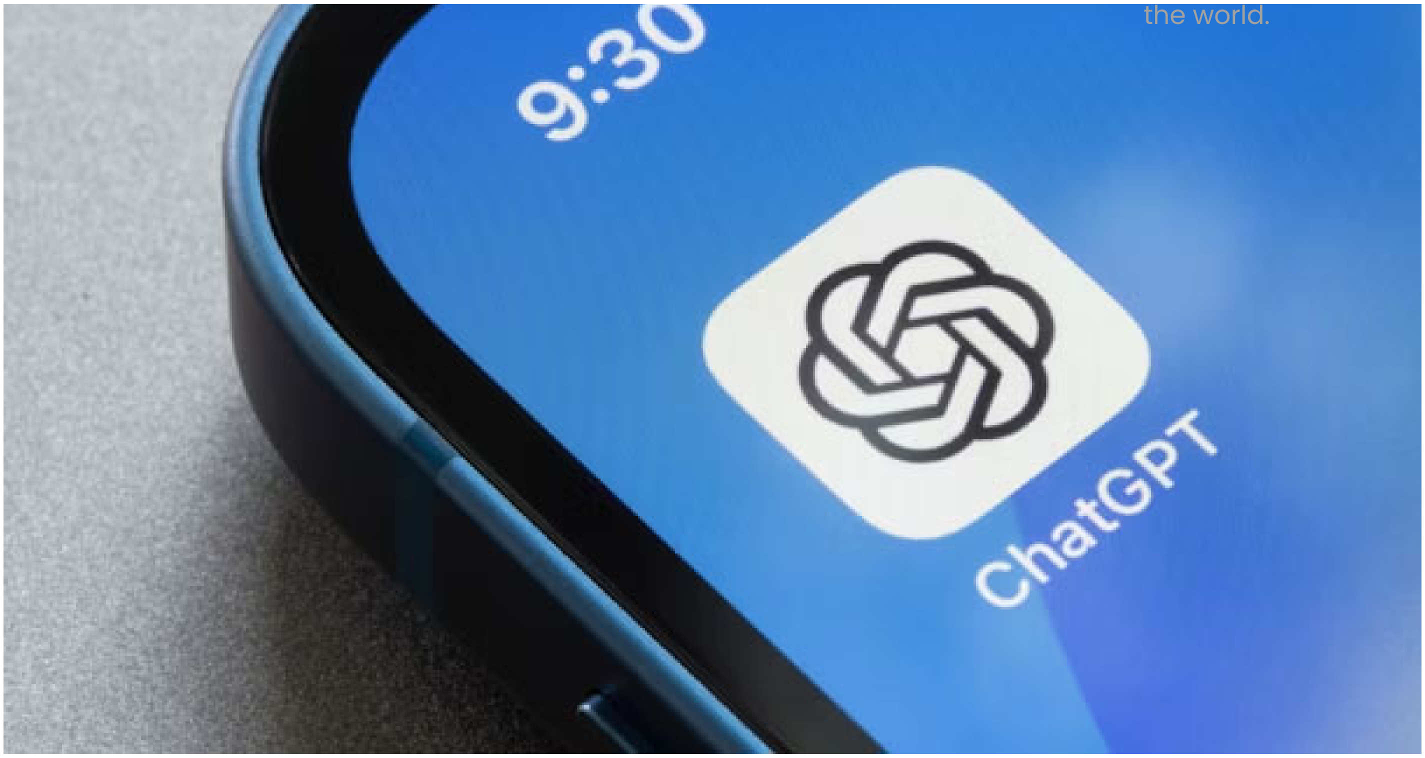
Share

By Webb Wright | NY Reporter

AUGUST 1, 2023 | 11 MIN READ

Listen to article 9 min 13 sec

While the technology is being hailed within the marketing industry for its ability to supercharge and supplement human creativity, it's also presenting some thorny legal questions.



ChatGPT is based upon a LLM called GPT-4, which is trained using vast amounts of data from the internet. / Adobe Stock

2023 could very well be remembered within the marketing industry as the Year of Generative AI.

Over the past several months, platforms like ChatGPT, Dall-E 2, Midjourney and Stable Diffusion have been making waves within the world of advertising for their ability to quickly and competently produce content from text-based user inputs. Some marketers have hailed generative AI as a complete paradigm shift. And at the most recent Cannes Lions festival – the ad industry's biggest annual event – the tech was the undisputed center of attention.

But generative AI has a glaring problem – one that's becoming increasingly difficult for marketers to ignore: it's opening up a messy and dangerous web of copyright concerns.

The problem with training LLMs

like OpenAI's GPT-4 and Google's LaMDA, for example, were trained from huge volumes of text culled from the internet. Through techniques like natural language processing and reinforcement learning, LLMs gradually develop the capability to mimic the information that's fed to them in a training dataset by producing 'original' text which convincingly appears as though it could've been composed by a human being (even if that text occasionally deviates from the truth).

As generative AI becomes increasingly powerful and accessible, a growing number of voices are rising in protest to what they view as the technology's flagrant disregard for copyright law.

A number of artists, for example, have publicly claimed that image-generating platforms like Midjourney and Stable Diffusion are plagiarizing their work. And in June, two lawsuits filed on behalf of a total of five authors – including the comedian Sarah Silverman – accused OpenAI and Meta of illegally using copyrighted book material to train LLMs.

The attorneys behind the class-action lawsuits, Joseph Saveri and Matthew Butterick, claim in their case briefing that the tech companies "copied" the authors' work "without consent, without credit, and without compensation." (Saveri and Butterick have also filed similar lawsuits against Stable Diffusion and the code-generating AI platform GitHub.)

Generative AI, Saveri and Butterick write in their new briefing, "is just human intelligence, repackaged and divorced from its creators."

The June lawsuits against OpenAI and Meta are just two examples from what is already becoming a long string of such cases made against the companies that are building generative AI.

"The basic question of whether or not an AI using copyrighted work constitutes copyright infringement is, for now, an open issue," says patent attorney Robert McFarlane. Ultimately, McFarlane believes that some uses of generative AI will be

ned to constitute copyright infringement while others won't. "These cases that are just starting now are going to try to draw that line," he says.

Columbia Law School professor Shyamkrishna Balganesh echoes that belief that the American legal system's eventual determination of whether or not the training of an LLM constitutes copyright infringement will almost certainly not be cut-and-dry. "The biggest impediment we have right now, in my view, is the assumption that everyone makes that there is a clear answer," he says, adding that "there's a lot of misplaced reliance" within the legal profession on the so-called "fair use" doctrine, a US law intended to limit the reach of copyright claims and allow for the legal and permissionless use of some copyrighted content.

In a foundational case for US fair use law, Authors Guild v Google, a federal court held in 2015 that the Google Book Search program – through which millions of copyrighted books were scanned and digitized without the authors' permission – did not violate US copyright law. The decision was later upheld by the US Supreme Court. In essence, the courts reasoned that Google was not attempting to "substitute" the original copies of the books through the digital versions and also that the tech company was in fact providing a legitimate public service by distributing information among the public and widening authors' readerships.

"A lot of lawyers for the AI industry strongly believe that the fair use doctrine coming out of [Authors Guild v Google] is going to protect the training purposes that are behind the ML model," Balganesh says. "Myself, I'm not sure that that's an open-and-shut case."

The courts could ultimately decide, for example, that the scanning and digitization of books for the purpose of online search is fundamentally different from a machine ingesting those same books in order to refine its capabilities. "There's a universe in which there's a difference [and] it may seem subtle, but I think it's a subtlety with a potentially significant variation," says Balganesh.

Commerciality – that is, the intention or lack thereof to make a profit – is also a salient issue here. To this point, Balganesh points to the recent Supreme Court decision in Andy Warhol Foundation for the Visual Arts Inc v Goldsmith, which held that Warhol's painting of the musician Prince, based on a photograph taken by Lynn Goldsmith, did not constitute fair use, primarily because the artist (who died in 1987) had created the

When considering the lawsuits that are being leveled against the tech companies that are developing generative AI models, Balganesh says that courts will need to assess: "Are you producing it for commercial purposes, or are you producing it for non-commercial purposes? OpenAI may well be different from Meta in terms of commerciality... that's why the belief that the fair use doctrine has a clear answer to the question [of whether or not using copyrighted material to train generative AI models] is probably a big mistake."

How might tech companies respond to the accusations of copyright infringement that are being leveled against them? One possible defense might be the argument that the content produced by LLMs is sufficiently different from the texts upon which they were trained so as to exonerate them from any such accusations.

Brenda Leong, an attorney who specializes in AI, compares this hypothetical scenario to a human painter who borrows from the style of a well-known artist: "I can paint something in the style of Van Gogh as long as I don't try to assert that it's by Van Gogh," she says. "I can't copy his exact picture, but I can paint in his style, and I can even copy his exact picture if I make enough changes to it. I can make a spoof, I can make a parody, I can make these different categories of reinterpretation of someone else's art and use that commercially."

The question of whether or not a machine can legally do the same thing, Leong says, is one that the courts will now have to grapple with.

Given the uncertain and still-evolving legal landscape which currently surrounds generative AI, how should marketers approach this technology?

Broadly speaking, in light of the fact that these are legal questions that are just beginning to be debated, the best thing that marketers can do at the moment is to pay attention to the relevant cases. “For now, marketers working with [generative AI] would be foolish not to keep their ears to the ground on legal challenges,” says Mark Penn, president and managing partner of the Stagwell Group.

The legal landscape surrounding the tech “is very fluid between lawsuits and regulation and it will take some time for the complexity of copyright and IP to get sorted out and unwind,” says Brian Yamada, chief innovation officer at VMLY&R. “It is critical to stay connected to both agency and client legal teams for any AI-forward work.”

If a brand partner is concerned about the associated legal risks of leveraging generative AI, “then it might be best to stay away from using models that are trained on copyrighted data,” says Mike Creighton, executive director of experience innovation at Instrument.

Enjoy a lunchtime read

Marketing

Soiled briefs: your parody ad won't make a mark, here’s the fix

Marketing

Less time at bars and pubs, more marathons: A snapshot of our 2024 leisure lives

Agencies

Ogilvy’s latest partnership tests how far strategists can trust an AI focus group

It’s also worth bearing in mind the current legal status of content that’s produced by generative AI. In a recently published document called Generative Artificial Intelligence

Marketina

Copyright Office recognizes copyright only in works 'created by a human being.'"

The document also notes that "works created by humans using generative AI could arguably be entitled to copyright protection, depending on the nature of human involvement in the creative process." But simply entering a text-based prompt, according to the document, will probably not constitute a sufficient degree of "human involvement" to be afforded copyright protection.

"This certainly affects client-agency relationships in which content is created under a work-for-hire agreement," says Paul Roetzer, founder and CEO of the Marketing AI Institute. "If agencies are using AI to generate content for clients, the client usually assumes they own the copyright for that content, but that may not be the case."

For more on the latest happenings in AI, web3 and other cutting-edge technologies, sign up for The Emerging Tech Briefing newsletter.

Technology Artificial Intelligence Generative AI

Industry insights

View all

Add your own content +

Remerge

Mobile marketing in 2024: Expert insights on what to expect

Depositphotos

What photos to choose for sales campaigns in 2024: 7 trends to explore

Tagger by Sprout Social

Only 28% of women occupy c-suite roles - here are 4 ways to change that

Trending

Marketing

Reuters Legal News

Ethical considerations in the use of AI

By Brad Hise, Esq., and Jenny Dao, Esq., Hanson Bridgett LLP

OCTOBER 2, 2023

The burgeoning use of artificial intelligence ("AI") platforms and tools such as ChatGPT creates both opportunities and risks for the practice of law. In particular, the use of AI in research, document drafting and other work product presents a number of ethical issues for lawyers to consider as they contemplate how the use of AI may benefit their practices. In California, as in other states, several ethics rules are particularly relevant to a discussion of the use of AI.

Although some ethical questions may lack clear answers, being mindful of these issues before integrating AI may help lawyers avoid issues in the future. This article will analyze AI questions through the lens of the California Rules of Professional Conduct.

A. Professional obligations and the California Rules of Professional Conduct

Lawyers have a professional duty to maintain professional standards and ensure their use of AI is compatible with their ethical obligations under the State Bar of California's Rules of Professional Conduct (the "Rules") and applicable law. The Rules are "intended to regulate professional conduct of lawyers" and are "binding upon all lawyers" licensed in California. CRPC 1.0(a). Some Rules are particularly relevant to a discussion of the use of AI in the legal profession.

1. Competence

California Rule of Professional Conduct 1.1 imposes on lawyers a duty of competence, which, among other things, requires a lawyer to apply the "learning and skill…reasonably necessary" for the representation of a client. CRPC 1.1(b). The comments to Rule 1.1 further explain that the duty of competence "include[s] the duty to keep abreast of the changes in the law and its practice, including the benefits and risks associated with relevant technology." CRPC 1, Comment [1]. The use of AI in the practice of law presents at least two competence issues to consider.

First, lawyers have an ethical duty to understand the risks and benefits the use of AI tools present for both lawyers and clients, and how they may be used (or should not be used) to provide competent representation to clients.

Second, lawyers should consider how they can incorporate AI tools into their practices without compromising the competent representation of their clients. Although AI can be a powerful tool, the use of AI tools may have catastrophic results for both lawyers and clients if lawyers fail to vet any outputs prior to using them in their work. For example, two attorneys were sanctioned by a New York federal judge for submitting a brief authored by AI that referenced nonexistent case law. (For more information, see here: https://bit.ly/3szT97D.)

Finally, as AI tools become more sophisticated and their use in the legal profession becomes more widespread, lawyers will need to consider whether the failure to use an available AI tool would itself be a failure to meet the duty of competence.

2. Communication with clients

Rule 1.2 imposes on lawyers a duty to communicate with their clients about the scope of the lawyer's representation, and Rule 1.4 requires a lawyer to consult with the client about how the lawyer intends to accomplish the client's objectives.

> *Can a lawyer ethically bill a client for the work that an AI tool performed? Can an AI tool have an hourly rate? And how would a lawyer account for the "time" the AI tool "expended" to perform a particular task?*

Accordingly, these Rules may require a lawyer to explain how and why the lawyer intends to use AI tools in the course of representing the client, and to discuss with the client such tools' associated benefits and risks. If a lawyer chooses not to use AI, that decision may also need to be communicated to the client.

3. Fees for legal services

Rule 1.5 establishes the ethical limitations on the reasonable fees a lawyer may charge a client.

Because the factors used in determining the reasonableness of a fee include time/labor, novelty of the issue, and customary fees, novel fee issues can arise if a lawyer employs AI tools to perform some tasks in his representation of a client. Can a lawyer ethically bill a client for the work that an AI tool performed? Can an AI tool have an hourly rate? And how would a lawyer account for the "time" the AI tool "expended" to perform a particular task?

Conversely, if a lawyer could use AI to perform certain tasks — such as completing the first draft of a routine document, or reviewing

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

a contract to ensure defined terms are used consistently — but elects not to do so and instead performs the tasks himself and bills his client for the work at the lawyer's standard hourly rate, has the lawyer charged the client an unconscionable fee in violation of Rule 1.5? The answers to these questions are not clear, but a lawyer may have an ethical obligation to employ available technology to provide legal services to a client more efficiently.

4. Confidentiality

The duty of confidentiality codified in Business & Professions Code section 6068(e)(1) and Rule 1.6 requires a lawyer to maintain as confidential all information the lawyer learns from a client in the course of representing that client, unless the client authorizes its disclosure.

Some AI tools do not guarantee the confidentiality of user inputs. For example, OpenAI, the creator of ChatGPT, discloses in its Terms of Service and related documents that a user's "conversations may be reviewed" by OpenAI employees to "improve [OpenAI's] system," and OpenAI explicitly warns users not to "share any sensitive information in [their] conversations." (See OpenAI FAQs here: https://bit.ly/3qXj1tm.) Further, OpenAI's Privacy Policy places the burden of maintaining confidentiality on users: "[Y]ou should take special care in deciding what information you send to us via [ChatGPT]." (See Section 5 of OpenAI's Terms of Use: https://bit.ly/3QZxI9W.)

In order to comply with Rule 1.6, it is important that lawyers ensure the AI tools they employ have implemented measures to protect client information. Lawyers should review the terms of use and privacy policies of an AI tool before using it, and only use a particular tool when the lawyer is confident that the client's confidential information is secure.

5. Supervision

Rule 5.1 imposes on more senior lawyers an obligation to ensure that more junior lawyers working under their supervision comply with the Rules of Professional Conduct. Rule 5.2 imposes on non-supervisory lawyers an obligation to comply with the Rules of Professional Conduct. Finally, Rule 5.3 imposes on law firm managers and supervisory lawyers a supervisory obligation with respect to non-lawyers.

Law firm management and supervising partners must ensure that subordinate lawyers and non-lawyers use AI tools in accordance with their professional obligations. Non-supervisory lawyers and non-lawyers have an ethical obligation to use AI tools consistent with the Rules of Professional Conduct and California law. Rules 5.1, 5.2 and 5.3 arguably also impose an obligation on lawyers to "supervise" the work of AI tools lawyers use in their representation of clients. This includes understanding which tasks are appropriate for AI tools and ensuring the accuracy of AI outputs.

B. Practical implications of a lawyer's ethical obligations

While a review of the Rules may assist lawyers in identifying potential issues in the ethical use of AI tools in their practices, the Rules also provide helpful guidance in identifying practical suggestions for incorporating AI into the practice of law.

Lawyers should exercise care when deciding whether a particular AI tool would provide useful assistance in the representation of a client. Lawyers may, at times, need to consult with technology experts to understand an AI tool, how it works, and whether it can be usefully deployed in a particular client matter. Lawyers should also clearly communicate with their clients about the use of AI in the representation, including the risks and benefits of AI.

AI tools may be used as a starting point in generating content, but AI-generated work product should never be presented as finished content or a lawyer's final product. Lawyers have a professional obligation to thoroughly review any AI-generated work product to ensure the results are accurate.

Lawyers should also be cautious when sharing client or firm data with AI tools. If the tool lacks robust confidentiality and data security, obtaining the client's informed written consent is essential before using it. Additionally, lawyers should verify if any third parties can access the data to avoid compromising the attorney-client privilege.

Finally, lawyers should not directly quote output from AI tools in work product sent to clients, opposing parties, or the courts. As discussed above, any AI outputs should be reviewed thoroughly before being incorporated into a preliminary draft or version of any attorney work product. This recommendation includes confirming the accuracy of any cases cited to support a particular argument.

About the authors

Brad Hise (L), partner and general counsel of **Hanson Bridgett LLP**, advises the firm's attorneys on conflicts of interest, legal ethics, and other professional responsibility and risk management issues. He is based in San Francisco and can be reached at BHise@hansonbridgett.com. **Jenny Dao** (R), member of the firm's land use practice group, helps clients navigate the complex legal landscape of land use and zoning law. Her work primarily focuses on land use entitlement, permit approvals, and compliance with local and state land use laws. She is based in Walnut Creek, California, and can be reached at JDao@hansonbridgett.com.

This article was first published on Reuters Legal News and Westlaw Today on October 2, 2023.

WORLD INTELLECTUAL PROPERTY REVIEW
wipr

AI-created scripts are not ready for prime time (yet)

Vasilyev Alexandr / shutterstock.com

Hollywood writers secured a deal preventing the use of GenAI but why were producers so ready to make the concession? Andy Stroud of Hanson Bridgett digs into the subplot.

From the advent of TV there have always been writers' rooms—the formerly smoke-filled but now mostly snack-filled spaces where writers gather to swap storylines, hone scripts, and practise the art of writing quality television.

Writers' rooms even survived the pandemic, when rooms became Zooms. However, is the writers' room now going the way of the television antenna? An abandoned relic of a bygone age made obsolete by new technology? Apparently not…yet.

One of the questions central to the recently resolved writers' strike was the role of artificial intelligence (AI) in the writing of future movie scripts and television series. Writers fear that they will soon be replaced by AI, which may be used to craft entire scripts or even television series, without the assistance or input of a professional writer.

That fear has been assuaged, at least temporarily, through the agreement reached between writers and producers. The new 2023 Minimum Benefits Agreement (MBA) between writers and producers closely regulates the use of AI in the writing of future productions.

AI-generated material is not to be considered either literary material or source material under the MBA. Neither is AI considered a writer under the MBA. The producers cannot require a writer to use AI software such as ChatGPT for their writing and a writer may only use AI with the approval of the producer and under strict guidelines.

What's in it for the producers?

Given the implications of AI as a significant labour-saving device for creating content, the question is why were the producers so willing to bargain away their right to use this new technology?

The answer, I believe, lies in the lack of protection the Copyright Act presently provides for AI-generated materials. Were a television series or movie to be written either solely or primarily through the use of AI software, then it would not be protected by copyright law and could be pirated with impunity.

This is because both the copyright office and the courts now agree that the protections of a copyright and the Copyright Act itself only apply to works created by humans. See, for example, *Naruto v Slater*, 888 F.3d 418, 420 (9th Cir. 2018) (Only humans have standing to pursue claims under the Copyright Act.); *Thaler v Perlmutter*, ___ F.Supp.3d_____, (2023 WL 5333236) ("United States copyright law protects only works of human creation".

Indeed, the Copyright Office now requires authors to “disclaim” for copyright purposes any part of their work that was generated by AI, so that part of the work cannot qualify for copyright protection.

Thus, just as AI cannot qualify as a “writer” because it is not human, so too an AI-generated work cannot qualify for copyright protection because it lacks human creation.

The Copyright Office recently demonstrated the implications of these decisions in its determination to deny registration to *Theatre D'Opera Spatial,* a visual work of art generated in part by AI, which was recently submitted for registration.

Although the work was well known because it won the Colorado State Fair’s fine art works competition in 2022, the Copyright Office denied registration because the work was generated by AI, and the author refused to disclaim the parts of the work that were AI-generated as opposed to his own work.

Consequently, the Copyright Office decided that, as the work contained more than a *de minimus* amount of AI content, it did not qualify for registration.

Likewise, under the current status of the copyright law, scripts that are primarily generated through AI would undoubtedly be denied copyright protection. This would mean that the scripts could be copied or used by anyone as they would essentially be in the public domain.

Moreover, although the television programme or movie created using an AI-generated script might qualify for copyright protection as a visual work, the characters and content of the work would presumably not qualify for protection because they were created through AI.

Humans still required

Hollywood, therefore, finds it best not to rely primarily on AI for generating creative works as the law presently stands, because the content of those works might not be subject to copyright protection.

Not coincidentally, this is almost exactly what was agreed to by both sides in the new MBA. AI cannot be used to write or rewrite literary materials and studios may not use scripts generated by AI as source materials.

Although a writer can use AI to generate ideas for scripts, they must advise the producer of that fact and only use AI under strict guidelines generated by the studios.

No doubt those guidelines serve to ensure that the AI input into the work is *de minimus* at most. In other words, under the MBA, human input is required at every step of the creative chain, mirroring the Copyright Office's present requirement for registration of a work that was generated in part by AI.

Like many IP practitioners, I was initially surprised that the producers did not insist that the old-fashioned writers' room now give way to the new AI computer room as a means of creating content at a greatly reduced cost.

However, when taking into account the present status of copyright law for AI-generated work, it seems clear that the producers were not giving much away at all.

Instead, they were doing as producers typically do, and protecting their significant investment in the work.

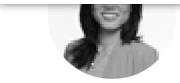
This is because, under the present state of the copyright law, AI-generated content is not ready for prime time. Yet.

Andy Stroud is a partner at Hanson Bridgett. He can be contacted at: AStroud@hansonbridgett.com

Infosecurity Magazine Home » Opinions » Data Privacy Week: Navigating Data Privacy in the Age of AI

OPINION 25 JAN 2024

Data Privacy Week: Navigating Data Privacy in the Age of AI



Associate, Hanson Bridgett

Batya Forsyth
Partner, Hanson Bridgett

Rob McFarlane
Partner, Hanson Bridgett

On October 30, 2023, the White House issued an Executive Order (EO) on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The EO marks a significant shift in the development of AI regulation and aims to create structured governance in sectors ranging from healthcare to national security.

In the realm of privacy, the EO seeks to strengthen AI data protection and advocates for legislation to protect personal data, with a particular focus on children. It further supports the development of privacy-preserving AI technologies and directs federal agencies to enhance privacy measures and evaluate data use, emphasizing the protection of American citizens' data privacy.

Global Perspectives and Parallel Developments

The EO on AI regulation is part of a wider international trend towards managing AI risks. The European Union (EU) with its General Data Protection Regulation (GDPR) and Asian countries like Japan and Singapore have made significant strides in AI data privacy. These global initiatives, reflecting a consensus on the need for coordinated AI regulation, offer insights and benchmarks for the US in its regulatory efforts.

The EU's AI Act

The EU is advancing in AI regulation with the development of the AI Act set to be the first comprehensive AI law globally. The Act focuses on mitigating risks in areas like healthcare and education, categorizing AI systems by risk levels. High-risk systems will face stringent rules, including risk mitigation and human oversight, while most AI applications are exempt from these strict requirements.

Key features of the AI Act include mandatory transparency and ethical standards for AI use. Companies must disclose AI interactions, especially those involving biometrics or emotions, and label AI-generated content like deepfakes. The EU is establishing a European AI Office to oversee compliance and enforcement, with significant fines for non-compliance.

The Act prohibits certain AI uses, such as indiscriminate facial image scraping and social scoring, but exempts military and defense AI systems. Its formal adoption is expected in early 2024, with varying compliance timelines for different AI system categories. The European Data Protection Supervisor (EDPS) will oversee AI systems within EU institutions, emphasizing risk prohibition and centralized enforcement.

The AI Act's relationship with the GDPR involves overlapping concerns, with AI systems processing personal data needing to comply with GDPR. The EU is considering revising GDPR to support AI innovation. Additionally, the European Commission has introduced model clauses for AI procurement to ensure AI Act compliance.

Overall, the EU's AI Act aims to balance innovation with fundamental rights and data privacy protection, establishing a comprehensive AI governance framework emphasizing transparency, ethics and accountability.

AI Data Privacy Regulation in Asia

The GDPR significantly influences data privacy regulations within Asia, with Asian countries are developing a variety of data protection frameworks. While there is a trend towards GDPR alignment, nations like South Korea, Japan, Singapore, and China show advancements in specific privacy areas like data security and localization. This variation presents challenges for global businesses in Asia, requiring adaptable yet localized data protection strategies.

Asian data protection laws often follow the 1980 Organization for Economic Cooperation and Development (OECD) Guidelines, focusing on principles like choice, notice, consent, data minimization, and cross-border transfer restrictions. However, implementation varies across countries, especially in consent definitions, breach notification mandates, and data subjects' rights.

Countries with established data protection laws, such as Japan, the Philippines, Singapore, and South Korea, have updated their legislation to include GDPR elements. China and Thailand have introduced comprehensive data protection laws influenced by GDPR. India and Vietnam, lacking comprehensive laws, have proposed GDPR-like bills.

With AI relying on extensive data, including sensitive information, the mandatory breach notification in countries like China, Japan, Singapore, and South Korea ensures transparency in AI data breaches. Furthermore, the incorporation of GDPR elements like extraterritorial scope and biometric data protection in Asian laws highlights the need for balancing AI innovation with privacy rights, and harmonizing AI data practices across diverse legal frameworks in the region.

Private Sector Response and Future Outlook

In the private sector, ethical AI practices are increasingly vital for compliance, consumer trust, and corporate responsibility. Companies are investing in advanced cybersecurity, data protection, and ethical AI development, a strategic move to stay competitive in the fast-evolving tech landscape.

The integration of AI into various aspects of life brings complex challenges and risks, especially concerning data privacy, AI biases, and user consent. High-profile incidents with Facebook, Clearview AI, and AI Dungeon illustrate these conflicts.

To tackle AI data privacy challenges, various companies are developing solutions to prevent sensitive data leakage into large language models (LLMs) like ChatGPT. These solutions typically include safe model training, excluding sensitive data, support for multi-party training, and protection against data collection through inference, using techniques like data redaction and tokenization.

Other firms provide similar data management software, such as Skyflow, Nightfall AI, Darktrace, Segment, and Data Grail.

Overall, private companies are navigating a challenging AI data privacy landscape, balancing extensive data needs with ethical, legal, and security concerns. This environment demands continuous vigilance, adaptability, and a commitment to responsible AI practices.

Conclusion

The White House's Executive Order marks a key advancement in AI regulation, emphasizing cybersecurity and privacy, particularly in healthcare and national security. It initiates a collaborative approach to develop AI standards and advocates for bipartisan data privacy laws.

Globally, this aligns with similar initiatives in the EU and Asia, influenced by the EU's GDPR. Concurrently, the private sector is focusing on ethical AI practices to navigate the evolving landscape of data regulation and AI technology.

Business & Practice
March 5, 2024, 2:10 AM PST

California Lawmaker’s Bill Weighs Rules on AI Usage for Lawyers

By Titus Wu

- Measure may look at disclosure requirements
- California bar passed AI usage guidance

A California lawmaker is exploring rules on how legal professionals use artificial intelligence—particularly the type that can generate text and other content on its own—when filing court documents.

Assemblymember Josh Lowenthal (D) introduced last month a measure (A.B. 2811) that would put in place disclosure and citation requirements around AI-assisted legal filings. Details on those requirements are still not available, said Guy Strahl, Lowenthal’s chief of staff, as his office is still working out specific language.

The bill comes amid debate and controversy over how AI will impact the legal sector. Already, some high-profile cases have captured the legal industry’s attention, such as New York lawyers submitting briefs citing non-existent cases fabricated by popular AI tool ChatGPT.

“There are multiple issues that need to be addressed” when lawyers use AI, said Bradford Hise, who advises attorneys on legal ethics at Hanson Bridgett. “This is a fascinating area, and it’s evolving very quickly.”

Precautionary Efforts

Most lawyers are already using some form of AI when prepping their work, Hise said. Legal research products like Westlaw or Bloomberg Law’s tools use the technology to help easily search for past cases or automate brief analyses, he added.

Questions arise when lawyers use generative AI like ChatGPT to completely do their work, such as writing briefs and other documents. It’s important if lawyers use such technology that they ensure everything produced is accurate, Hise said, from the text to the citations to the legal conclusion. The AI technology has the potential to “hallucinate,” or generate outputs that don’t make sense, such as making up court cases.

Across the nation, some policymakers are taking initial steps to keep inaccurate AI from affecting lawyers and their clients negatively. A policy memo for a New York City borough’s office, for instance, bans generative AI use for dispensing legal advice, arguing AI models lack an understanding of up-to-date legal principles.

In California and some other states, state bar associations have recognized the growing prevalence of the technology and are addressing the topic. The California State Bar last November issued guidelines, making it presumably the first regulatory agency for lawyers to enact AI guidelines.

The guidance calls for lawyers to disclose AI use to clients and to ensure a human is reviewing all AI-generated outputs. Anything produced should be examined for inaccuracy and bias, according to the document, and there should not be an overreliance on such tools. The bar noted this guidance is a “living document” that could be updated as the technology evolves.

The guidance is similar to what Lowenthal intends to address with disclosures and citation accuracy in his bill. In fact, the guidance called on the state bar to work with the state legislature on exploring law changes, including whether legal generative AI products need to be regulated.

California State Bar spokesperson Rick Coca said the bar isn’t involved and hasn’t taken a position on the Lowenthal effort.

Not Necessary?

Some legal analysts question if the bill is necessary. They note that there are already mechanisms in place that punish attorneys who submit false or inaccurate information, including from AI, such as sanctions and fines from a judge or a malpractice lawsuit from a client.

“There’s certainly a problem with incompetent lawyers. It’s just not a problem that the bill will solve,” said Eugene Volokh, a law professor at the University of California, Los Angeles.

Volokh also questioned whether disclosure requirements would have any effect. Usage of AI could become as ubiquitous as, for example, lawyers utilizing summer law students in preparing a brief or other legal document.

“So imagine there was a rule that said you have to disclose whether anybody who’s not a member of the bar worked on the briefs,” said Volokh. “All of these briefs would have this one sentence and the judges will ignore it.”

Ultimately, some attorneys contend it’s better to have the law profession be regulated by lawyers and judges, not legislators. State statute is much harder to change to keep up to pace with AI’s rapid evolution, they argued.

“I would be hesitant to support changes that address a technology that may, in fact, be superseded in two years, six months, whatever time frame,” said Hise. “I think it’s probably better for lawyers to look at technology through the lens of our existing rules of professional conduct.”

To contact the reporter on this story: Titus Wu in Sacramento, Calif. at twu@bloombergindustry.com

To contact the editors responsible for this story: Bill Swindell at bswindell@bloombergindustry.com; Fawn Johnson at fjohnson@bloombergindustry.com

Business & Practice
March 7, 2024, 2:30 AM PST

Law Firms Aren't Behind the Generative AI Adoption Curve—Yet

By Roy Strom

Column

Related Stories

Insurers Seek Drastic Haircut To $185 Million Quinn Emanuel Fee
March 6, 2024, 9:41 AM PST

Business Is Booming For DEI Lawyers As Firms Ask 'What's Legal?'
March 5, 2024, 2:00 AM PST

From SPAC Dreams To Riviera Mirage: How Lottery.Com Imploded (1)
March 4, 2024, 2:01 AM PST

Musk Taps '$5 Billion Man' Chu For OpenAI, Altman Lawsuit (1)
March 1, 2024, 8:43 AM PST

Associates Can Say 'Domo Arigato' For AI That Isn't Job Killer
December 14, 2023, 2:30 AM PST

More Stories (1)

Welcome back to the Big Law Business column. I'm Roy Strom, and today we look at how law firms stack up to other companies deploying generative AI tools. Sign up to receive this column in your Inbox on Thursday mornings.

A lot has happened since the world met ChatGPT in late 2022. It's dominated headlines, minted billions (or trillions) in the stock market, and, in the surest sign yet that it's captured the zeitgeist, even generated more work for Elon Musk's lawyers.

It might feel like the AI revolution is well underway. But for all the excitement, generative AI has not yet transformed many businesses. In fact, very few companies use it to make products or sell services and only a relative handful of companies expect they will do so in the near future.

This puts lawyers—notoriously maligned as something near Luddites—in a rare spot: They might be ahead of the curve on adopting a new technology. At the very least, it's hard to argue law firms are lagging the broader economy when it comes to putting AI tools to good use.

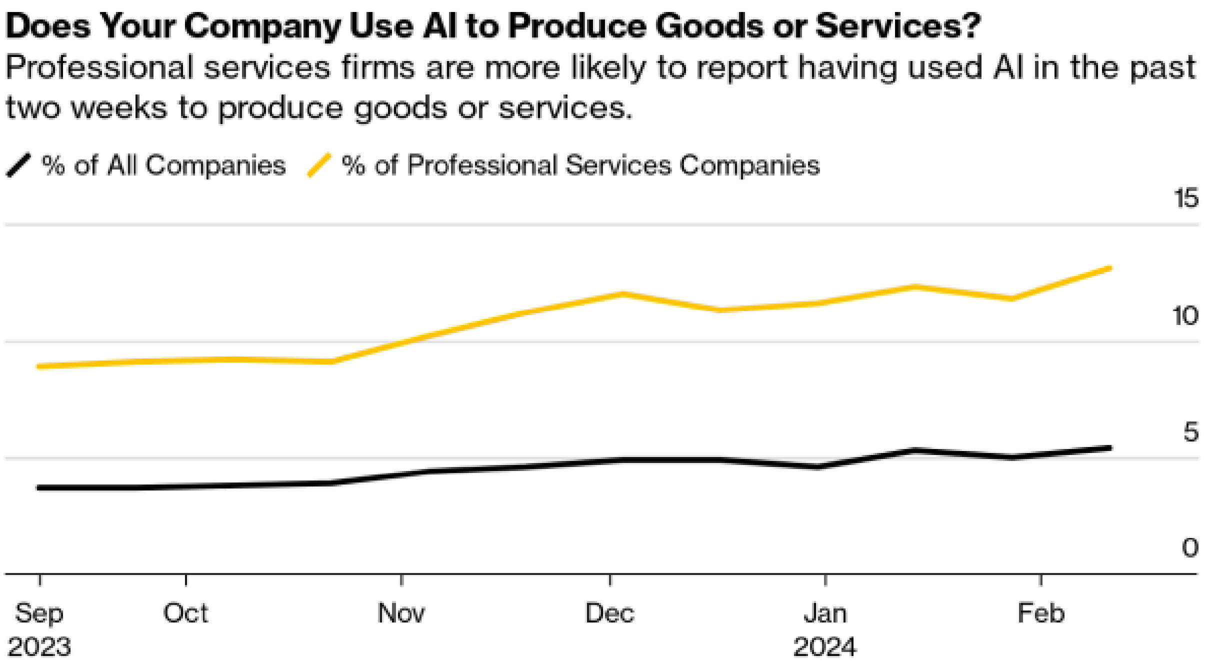
In February, a mere 5.4% of American companies said that within the past two weeks they had used AI to produce goods or services, according to data from the US Census Bureau, which began asking about companies' AI-fueled products in September. (Some 28,000 companies responded to the Census questionnaire in February.)

Professional services companies, which includes law firms, were more likely to have put AI to good use: 13.1% of such businesses told the Census Bureau they'd used AI to produce goods or services in February.

While those numbers are not lawyer-specific, they are roughly in-line with a Bloomberg Law survey last year that found 7% of lawyers had used AI to perform a work task.

The Census Bureau also asks companies whether they will be using AI to produce products in the next six months. Only slightly more companies answered affirmatively: 6.6% of all companies and 16.1% of professional services firms.

But across the economy, fewer companies are answering "no," suggesting they're at least tinkering with AI.



Does Your Company Use AI to Produce Goods or Services?

Professional services firms are more likely to report having used AI in the past two weeks to produce goods or services.

Source: US Census Bureau

Bloomberg Law

Law firms are still finding their footing. But examples abound of firms who say they are using AI to help clients.

Allen & Overy said around 3,500 of its lawyers had asked an AI program around 40,000 queries for their day-to-day client work—and that was over a year ago. DLA Piper has paired data scientists with lawyers to use AI to test large language models for bias or legal problems. Dechert has rolled out a suite of internally built generative AI offerings branded DechertMind.

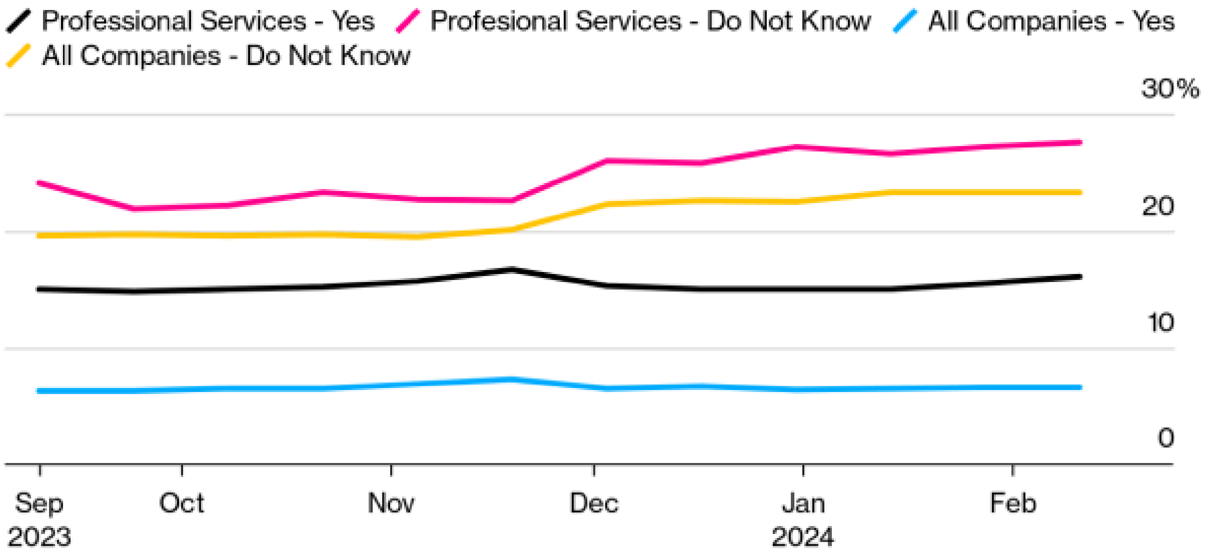
Blake Rooney, chief information officer at Husch Blackwell, said his job has changed significantly in the past 18 months. Used to an internal role, he’s now getting face time with clients to talk about how his law firm and its data science team can use AI to provide better services. He was in client meetings in Minneapolis last week and in Nashville the week prior.

Rooney’s firm has had plenty of projects for AI pop up in recent months. In one example, a client facing a deadline to file a temporary restraining order asked the firm to pore over hundreds of voicemails. The firm used an AI program to transcribe and index the messages, turning the project around the same day, Rooney said.

“We’re starting to see a good number of projects like that where if it was a human effort it would be enormous, but using technology we can get good answers in good short order,” Rooney said.

Will Your Company Use AI In the Next Six Months?

Many companies still don't know whether they will use AI to produce goods or services in the next six months.



Source: US Census Bureau

Bloomberg Law

Companies that are curious about AI tools are often turning to their legal departments as a place to try new products, said Richard Punt, global leader of Deloitte Legal.

“There’s quite an interesting subset of companies who are saying, ‘Can we find something that’s more back-office we can practice on?’” Punt said. “And it’s surprising how often legal is the area that they want to practice. You’re seeing legal [departments] come to the front of the queue inside companies.”

Lawyers are constrained in their use of AI by ethics rules and privacy concerns. Buying AI tools can also be expensive, which could prevent smaller firms from making early investments.

That would also be like the broader economy. Companies with 250 or more employees are more likely than smaller businesses to have used AI to sell products or services, the Census data show.

Warren Hodges, who leads an AI task force at 200-lawyer Hanson Bridgett, said his firm has stayed up-to-date on generative AI tools. It’s studied the ethics of using AI for client work, and Hodges said the firm’s lawyers are convinced it can provide “incredibly powerful” solutions.

The firm is “not under the illusion” that it won’t eventually invest in something, Hodges said, but for now it’s taken a wait-and-see approach.

“The products will get better and cheaper over time, and it’s not easy to roll out anything new companywide,” Hodges said. “Every company faces that and law firms are no different.”

Staying Ahead

There’s no guarantee law firms will succeed in adopting AI tools. And it will no doubt present challenges to law firms’ hourly billing model. But they’re at least off to a decent start relative to the rest of the business world.

One way to ensure they stay ahead of the curve is to educate more employees on generative AI tools.

Law firms would be wise to invest more in training programs like those offered through Coursera, an online education platform, said Tracey George, a Vanderbilt Law School professor who oversees an interdisciplinary generative AI team for the university.

She said many of the most sophisticated technology companies provide Coursera classes for employees, many of which are free. She has particular insight into popular GenAI classes offered by Vanderbilt, and she said few if any law firms have used them.

Using a similar model for pro bono work, George suggests law firms provide a billable hour credit for lawyers spending time learning about AI. Law firms that pledge their lawyers would spend 40 or 50 hours learning about the technology would send a strong signal to clients that they’re serious about performing work more efficiently, she said.

“The equivalent of one work week would make a difference,” she said.

Worth Your Time

On Legal Fees: Objectors to a $185 million fee won by Quinn Emanuel are seeking to drastically slash the award to roughly $12 million to $23 million. The most recent court filing in the long-running dispute also shed light on a judgment preservation insurance policy Quinn Emanuel purchased to protect the award.

On SPACs: Nicola White details the travails of Lottery.com Inc., which she reports came to represent “all the hubris and excesses of the special purpose acquisition company era.” The company had phantom revenues, multiple CEOs hired and fired, accusations of forged documents, an alleged check-kiting scheme, and more.

On DEI: Business is booming for DEI lawyers as companies try to figure out what’s legal in wake of the Supreme Court’s ruling, Bloomberg’s Simone Foxman reports.

That’s it for this week! Thanks for reading and please send me your thoughts, critiques, and tips.

To contact the reporter on this story: Roy Strom in Chicago at rstrom@bloomberglaw.com

To contact the editor responsible for this story: Alessandra Rafferty at arafferty@bloomberglaw.com

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

For Release

FTC Proposes New Protections to Combat AI Impersonation of Individuals

Agency finalizes rule banning government and impersonation fraud and seeks to extend protections to individuals

February 15, 2024

Tags: Consumer Protection | Bureau of Consumer Protection | Imposter | government | deceptive/misleading conduct | Technology | Advertising and Marketing | Tech | Artificial Intelligence

Give Feedback

The Federal Trade Commission is seeking public comment on a supplemental notice of proposed rulemaking that would prohibit the impersonation of individuals. The proposed rule changes wou extend protections of the new rule on government and business impersonation that is being finalized by the Commission today.

The agency is taking this action in light of surging complaints around impersonation fraud, as well as public outcry about the harms caused to consumers and to impersonated individuals. Emerging technology – including AI-generated deepfakes – threatens to turbocharge this scourge, and the FTC is committed to using all of its tools to detect, deter, and halt impersonation fraud.

The Commission is also seeking comment on whether the revised rule should declare it unlawful for a firm, such as an AI platform that creates images, video, or text, to provide goods or services that they know or have reason to know is being used to harm consumers through impersonation.

“Fraudsters are using AI tools to impersonate individuals with eerie precision and at a much wider scale. With voice cloning and other AI-driven scams on the rise, protecting Americans from impersonator fraud is more critical than ever,” said FTC Chair Lina M. Khan. “Our proposed expansions to the final impersonation rule would do just that, strengthening the FTC's toolkit to address AI-enabled scams impersonating individuals."

The supplemental notice of proposed rulemaking is being issued in response to comments received during the public comment period on the government and business impersonation rule that pointed to the additional threats and harms posed by impersonation of individuals. As scammers find new ways to defraud consumers, including through AI-generated deepfakes, this proposal will help the agency deter fraud and secure redress for harmed consumers.

Final Rule on Government and Business Impersonation

In addition to the supplemental notice, the FTC has finalized the Government and Business Impersonation Rule, which gives the agency stronger tools to combat scammers who impersonate businesses or government agencies, enabling the FTC to directly file federal court cases aimed at forcing scammers to return the money they made from government or business impersonation scams. This is particularly important given the Supreme Court's April 2021 ruling in AMG Capital Management LLC v. FTC, which significantly limited the agency's ability to require defendants to return money injured consumers.

Government and business impersonation scams have cost consumers billions of dollars in recent years, and both categories saw significant increases in reports to the FTC in 2023. The rule authorizes the agency to fight these scams more effectively.

For example, the rule would enable the FTC to directly seek monetary relief in federal court from scammers that:

- **Use government seals or business logos** when communicating with consumers by mail or online.
- **Spoof government and business emails and web addresses**, including spoofing ".gov" email addresses or using lookalike email addresses or websites that rely on misspellings of a company's name.
- **Falsely imply government or business affiliation** by using terms that are known to be affiliated with a government agency or business (e.g., stating "I'm calling from the Clerk's Office" to falsely imply affiliation with a court of law).

The publication of the final rule comes after the two rounds of public comment in response to an advance notice of proposed rulemaking issued in December 2021, a notice of proposed rulemaking issued in September 2022, and an informal hearing in May 2023.

The Commission vote to issue the final rule and the supplemental notice of proposed rulemaking and to publish them in the Federal Register was 3-0. Chair Lina M. Khan issued a separate statement that was joined by Commissioners Rebecca Kelly Slaughter and Alvaro M. Bedoya.

Both items will appear in the Federal Register shortly. The final rule on government and business impersonation will become effective 30 days from the date it is published in the Federal Register. The public comment period for the SNPRM will be open for 60 days following the date it is published in the Federal Register, and instructions for how to comment will be included in the notice.

The Federal Trade Commission works to promote competition and protect and educate consumers. The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. Learn more about consumer topics at consumer.ftc.gov, or report fraud, scams, and bad business practices at ReportFraud.ftc.gov. Follow the FTC on social media, read consumer alerts and the business blog, and sign up to get the latest FTC news and alerts.

Press Release Reference

FTC Proposes New Rule to Combat Government and Business Impersonation Scams

Contact Information

Contact for Consumers

FTC Consumer Response Center
877-382-4357
https://reportfraud.ftc.gov

Media Contact

Jay Mayfield
Office of Public Affairs
202-326-2656

Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act[1]

The increasing use of consumers' biometric information and related marketing of technologies that use or purport to use biometric information ("biometric information technologies")[2] raise significant concerns with respect to consumer privacy, data security, and the potential for bias and discrimination. The Federal Trade Commission is committed to combatting unfair or deceptive acts related to the collection and use of consumers' biometric information and the marketing and use of biometric information technologies.

As used in this document, the term "biometric information" refers to data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body. Biometric information includes, but is not limited to, depictions, images, descriptions, or recordings of an individual's facial features, iris or retina, finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern). Biometric information also includes data derived from such depictions, images, descriptions, or recordings, to the extent that it would be reasonably possible to identify the person from whose information the data had been derived. By way of example, both a photograph of a person's face and a facial recognition template, embedding, faceprint, or other data that encode measurements or characteristics of the face depicted in the photograph constitute biometric information.

Recent years have seen a proliferation of biometric information technologies. For instance, facial, iris, or fingerprint recognition technologies collect and process biometric information to identify individuals. Other biometric information technologies use or purport to use biometric information in order to determine characteristics of individuals, ranging from the individuals' age, gender, or race to the individuals' personality traits, aptitudes, or demeanor. Many biometric information technologies are developed using machine learning or similar data-driven processes that require large quantities of biometric information for "training" or testing purposes.

The Commission has been analyzing consumer protection issues related to biometric information for over a decade. Among other examples,[3] in 2011, as the commercial use of facial

[1] This Policy Statement does not confer any rights on any person and does not operate to bind the FTC or the public. In any enforcement action, the Commission must prove the challenged act or practice violates one or more existing statutory or regulatory requirements. In addition, this Policy Statement does not preempt federal, state, or local laws. Compliance with those laws, however, will not necessarily preclude Commission law enforcement action under the FTC Act or other statutes. Pursuant to the Congressional Review Act (5 U.S.C. § 801 et seq.), the Office of Information and Regulatory Affairs designated this Policy Statement as not a "major rule," as defined by 5 U.S.C. § 804(2).

[2] In some contexts, the terms "biometrics" or "biometric technologies" have been used to refer specifically to technologies that are used to identify individuals. We use the term "biometric information technologies" to refer to the broader category of all technologies that use or purport to use biometric information for any purpose.

[3] *See, e.g.*, Press Release, FTC, *FTC to Host Identity Authentication Workshop* (Feb. 21, 2007) https://www.ftc.gov/news-events/news/press-releases/2007/02/ftc-host-identity-authentication-w (announcing a public workshop on topics including biometrics and other emerging authentication technologies); *You Don't Say: An FTC Workshop on Voice Cloning Technologies*, FTC (Jan. 28, 2020), https://www.ftc.gov/news-events/events/2020/01/you-dont-say-ftc-workshop-voice-cloning-technologies.

recognition technology began to take off, the FTC hosted a public workshop, "Face Facts: A Forum on Facial Recognition Technology."[4] The workshop brought together stakeholders from government, academia, and industry to discuss the then-current capabilities and commercial uses of facial recognition technology, as well as potential consumer benefits of and privacy and security concerns about such technology. Following the workshop, in 2012, the FTC published a report entitled "Facing Facts: Best Practices For Common Uses of Facial Recognition Technologies."[5]

Since 2012, some biometric information technologies, such as facial recognition technology, have made significant advances. For example, NIST found that between 2014 and 2018, facial recognition became 20 times better at finding a matching photograph from a database.[6] Such improvements are due in significant part to advancements in machine learning,[7] along with data collection, storage, and processing capabilities sufficient to support the use of these technologies.[8] Simultaneously, many biometric information technologies have become less expensive to deploy.[9] Owing in part to these developments, the use of biometric information technologies is increasingly pervasive. For example, the use of facial recognition and other biometric information technologies in physical locations – such as retail stores, arenas, airports, and other venues – is reportedly growing.[10]

[4] FTC, FACE FACTS: A FORUM ON FACIAL RECOGNITION TECHNOLOGY (Dec. 8, 2011), https://www.ftc.gov/news-events/events/2011/12/face-facts-forum-facial-recognition-technology.

[5] FTC, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (Oct. 2012), https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies. Recommendations in this report remain relevant, such as reasonable data security protections for biometric information and appropriate data retention and disposal policies and procedures.

[6] NAT'L INSTITUTE FOR STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 6 (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf; *See also* NIST, Press Release, *NIST Evaluation Shows Advance in Face Recognition Software's Capabilities* (Nov. 30, 2018) https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.

[7] *See id.*

[8] *See* A.K. Jain et al., 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters 79 (2016) 100 (stating that "exponential improvements in computing and storage have enabled the deployment of more powerful algorithms to process the captured biometric data" and discussing how, "cloud-based biometrics can facilitate rapid analytics (e.g., recognizing a face using a smartphone camera, where the phone accesses the cloud).")

[9] *See id.* ("[E]xponential improvements in the performance and cost of processors and memory have already played a dominant role in the development of better biometric sensors. . . . In the case of biometric recognition, the direct impact of the rapid improvements in [integrated circuits] is the development of smaller, cheaper, and higher quality biometric sensors.").

[10] *See*, *e.g.*, National Retail Federation and Loss Prevention Research Council, *2022 Retail Security Survey: The State of National Retail Security and Organized Retail Crime*, 17, https://nrf.com/research/national-retail-security-survey-2022 (stating that 12.3% of respondents were implementing or planning to implement facial recognition for loss prevention); *Fast, Frictionless Biometric Payments Gaining Ground in Grocery Stores*, PYMNTS (May 24, 2022) https://www.pymnts.com/news/retail/2022/grocery-stores-will-be-big-winners-this-holiday-season/; Aaron Mok, *These 16 US airports are reportedly testing facial recognition technology on passengers that could roll out nationwide next year*, BUSINESS INSIDER (Dec. 6, 2022) https://www.businessinsider.com/these-16-us-airports-are-reportedly-testing-facial-recognition-tech-2022-12; Kashmir Hill and Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, NYTIMES (Dec. 22, 2022) https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html; Randy Wimbley and David Komer, *Black teen kicked out of skating rink after facial recognition camera misidentified her*,

During this same time period, the use of facial recognition and other biometric information technologies and the risks they pose have been the focus of significant public scrutiny and concern both in the U.S.[11] and abroad.[12] U.S. states and localities have passed laws specifically focused on regulating the commercial use of facial recognition and other biometric information technologies.[13] The requirements in these laws vary – for example, banning the use of facial recognition in certain locations,[14] requiring signs at the entrances of commercial establishments that collect biometric identifiers,[15] or requiring consent to collect biometric information.[16] In 2019 and 2021, the Commission also brought enforcement actions against companies that allegedly misrepresented their use of facial recognition technology.[17]

Consumers, businesses, and society now face new and increasing risks associated with the collection and use of biometric information. For example, biometric information can be used for the production of counterfeit videos or voice recordings (so-called "deepfakes") that would allow bad actors to convincingly impersonate individuals in order to commit fraud or to defame or harass the individuals depicted.[18] Large databases of biometric information may also be attractive targets for malicious actors because of the information's potential to be used for other

FOX2DETROIT (July 14, 2021) https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her.

[11] *See*, *e.g.*, *Privacy in the Age of Biometrics: Hearing Before the Subcomm. On Investigations and Oversight of the H. Comm. On Science, Space, and Technology* (2022), https://www.congress.gov/event/117th-congress/house-event/114964?s=1&r=8; *Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy: Hearing Before the House Committee on Oversight and Government Reform* (2020), https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110380; Rebecca Koenig, *New Advocacy Campaign Calls for Banning Facial Recognition on College Campuses*, EDSURGE (Jan. 22, 2020), https://www.edsurge.com/news/2020-01-22-new-advocacy-campaign-calls-for-banning-facial-recognition-on-college-campuses.

[12] *See*, *e.g.*, *Proposal for a Regulation Laying Down Harmonized Rule on Artificial Intelligence*, European Commission, 2021 O.J. (C 206), https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence; Global Privacy Assembly, *Adopted Resolution on Facial Recognition Technology*, (2020), https://edps.europa.eu/sites/default/files/publication/final_gpa_resolution_on_facial_recognition_technology_en.pdf

[13] *See*, *e.g.*, Washington Biometric Privacy Protection Act, Wash. Rev. Code § 19.375 (2022) (effective July 23, 2017); Prohibit the Use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City of Portland, PORTLAND, OR., CITY CODE Chapter 34.10 (2022) (effective Jan. 1, 2021); Biometric Identifier Information, NEW YORK, N.Y., ADMIN. CODE §§ 22-1201 – 1205 (2023) (effective July 9, 2021). Even prior to 2012, two states, Illinois and Texas, had enacted biometric privacy laws. *See* Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14 (effective Oct. 3, 2008); Texas Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code § 503.001 (effective Apr. 1, 2009). Additionally, states' comprehensive privacy laws address biometric information. *See, e.g.*, Colorado Privacy Act, 2021 Colo. Legis. Serv. Ch. 483 (S.B. 21-190) (West) (effective July 1, 2023).

[14] PORTLAND, OR., CITY CODE Chapter 34.10 (prohibiting use of face recognition technologies by private entities in places of public accommodation).

[15] NEW YORK, N.Y., ADMIN. CODE § 22-1202(a).

[16] 740 Ill. Comp. Stat. 14/15(b).

[17] Complaint, *In re Everalbum*, FTC File No. 1923172 (May 6, 2021); Complaint, *United States v. Facebook*, No. 19-cv-2184 (D.D.C. July 24, 2019).

[18] For example, in 2020, the Commission hosted a workshop to address the potential benefits and risks to consumers of technology that allows researchers to create a near-perfect voice clone with less than a five second recording of a person's voice. FTC, You Don't Say: An FTC Workshop on Voice Cloning Technologies (Jan. 28, 2020), https://www.ftc.gov/news-events/events/2020/01/you-dont-say-ftc-workshop-voice-cloning-technologies.

illicit purposes, including to achieve further unauthorized access to devices, facilities or data.[19] These issues pose risks not only to individual consumers, but also to businesses and society.[20]

Even outside of fraud, uses of biometric information or biometric information technology can pose significant risks to consumers. For instance, using biometric information technologies to identify consumers in certain locations could reveal sensitive personal information about them—for example, that they have accessed particular types of healthcare, attended religious services, or attended political or union meetings.[21] Moreover, without clear disclosures and meaningful choices for consumers about the use of biometric information technologies, consumers may have little way to avoid these risks or unintended consequences of these technologies.[22]

Some technologies using biometric information, such as facial recognition technology, may perform differently across different demographic groups in ways that facilitate or produce discriminatory outcomes. For example, research published by the National Institute of Standards and Technology (NIST) found that many facial recognition algorithms produce significantly more false positive "matches" for images of West and East African and East Asian faces than for images of Eastern European faces.[23] The research also found rates of false positives to be higher

[19] *See*, *e.g.*, Joseph Cox, *How I Broke Into a Bank Account With an AI-Generated Voice*, Motherboard, VICE (Feb. 23, 2023), https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice; Parmy Olson, *Faces Are the Next Target for Fraudsters*, WALL STREET JOURNAL (July 7, 2021), https://www.wsj.com/articles/faces-are-the-next-target-for-fraudsters-11625662828 (reporting, among other things, the successful hack of a Chinese facial recognition system by fraudsters who uploaded videos they had created from high-definition photographs purchased on the black market). Researchers have reportedly demonstrated techniques for replicating and using non-face biometric identifiers such as fingerprints to circumvent access controls. *See*, *e.g.*, Alex Hern, *Hacker fakes German minister's fingerprints using photos of her hands*, THE GUARDIAN (Dec. 30, 2014), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands. Unauthorized access could also be achieved using synthetic identifiers created by combining biometric information about a large number of individuals. *See* Philip Bontrager et al., *DeepMasterPrint: Generating Fingerprints for Presentation Attacks* (2017), https://www.researchgate.net/publication/317061803_DeepMasterPrint_Generating_Fingerprints_for_Presentation_Attacks.

[20] *See, e.g.*, 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters 79 (2016) 80–105 (discussing that "biometric system[s] may be vulnerable to a number of security threats . . . which may eventually affect the security of the end application."); Bobby Chesney and Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,* 107 California Law Review 1753, 1758 (2018) (discussing that some harms of deepfakes may be "distortion of policy debates, manipulation of elections, erosion of trust in institutions, exacerbation of social divisions, damage to national security, and disruption of international relations.").

[21] *See* FTC, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES, *supra* n.4, at ii (recommending that businesses consider the sensitivity of information that may be collected by facial recognition systems in light of the locations in which the systems operate).

[22] *See generally* FTC, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES, *supra* n.4, at iii (summarizing recommendations about providing clear notice and choices to consumers about the use of facial recognition technology).

[23] *See* FRVT Demographic Effects in Face Recognition, NAT'L INSTITUTE FOR STANDARDS AND TECH., https://pages.nist.gov/frvt/html/frvt_demographics.html (last accessed Aug. 31, 2022); NAT'L INSTITUTE FOR STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 8: SUMMARIZING DEMOGRAPHIC DIFFERENTIALS (2022), https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf; NAT'L INSTITUTE FOR STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 2 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.

in women than men, and in the elderly and children compared to middle-aged adults.[24] Demographic differentials may be even more pronounced when analyzed intersectionally (e.g., when comparing light-skinned males to dark-skinned females, rather than simply males to females and light-skinned subjects to dark-skinned subjects).[25] Similarly, some biometric information technologies, such as those that process facial images or voice recordings, may be particularly prone to error when the subject of the analysis is a person with a disability.[26] In light of this potential for bias, such technologies can lead or contribute to harmful or unlawful discrimination. This is particularly concerning when such technologies are used to determine whether consumers can receive important benefits and opportunities or are subject to penalties or less desirable outcomes. For example, if biometric information technologies are used to provide access to financial accounts, a false negative may result in the consumer being denied access to their own account, whereas a false positive may result in an identity thief gaining access to the account.[27] If biometric information technologies are used for security surveillance, false positives may result in individuals being falsely accused of crimes, subjected to searches or questioning, or denied access to physical premises.

In light of the evolving technologies[28] and risks to consumers, the Commission sets out below a non-exhaustive list of examples of practices it will scrutinize in determining whether companies collecting and using biometric information or marketing or using biometric information technologies are complying with Section 5 of the FTC Act.[29]

[24] *Id.*

[25] *See, e.g.,* Joy Buolamwini and Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proceedings of Machine Learning Research 1, 11 (2018) (assessing commercial gender classification systems and finding that all three performed worst for females with darker skin tones).

[26] *See, e.g.*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, EEOC-NVTA-2022-2, THE AMERICANS WITH DISABILITIES ACT AND THE USE OF SOFTWARE, ALGORITHMS, AND ARTIFICIAL INTELLIGENCE TO ASSESS JOB APPLICANTS AND EMPLOYEES (2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence (noting the potential that technologies analyzing the voice will be less accurate for individuals with speech impediments); SELIN E. NUGENT ET AL., INST. FOR ETHICAL A.I., RECRUITMENT AI HAS A DISABILITY PROBLEM: QUESTIONS EMPLOYERS SHOULD BE ASKING TO ENSURE FAIRNESS IN RECRUITMENT 12 (2020) (noting practical considerations that may affect the accuracy of facial analysis technology for individuals with certain disabilities).

[27] *See generally*, Joseph Cox, *How I Broke Into a Bank Account With an AI-Generated Voice*, Motherboard, VICE (Feb. 23, 2023), https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice.

[28] In some instances, biometric information technologies may utilize algorithms and/or artificial intelligence. The guidance below is consistent with and builds on previous publications by the Commission and Commission staff on those topics. *See, e.g.*, FTC, COMBATTING ONLINE HARMS THROUGH INNOVATION (June 2022); FTC, BIG DATA A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (Jan. 2016); Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC: BUS. BLOG (Apr. 19, 2021) https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai; Andrew Smith, *Using Artificial Intelligence and Algorithms,* FTC: BUS. BLOG (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms.

[29] Other laws and regulations enforced by the Commission, including but not limited to the Children's Online Privacy Protection Act (15 U.S.C. §§ 6501–6506) and its implementing Rule (16 C.F.R. Part 312), the Health Breach Notification Rule (16 C.F.R. Part 318), and the Gramm-Leach-Bliley Act's Safeguards Rule (16 C.F.R. Part 314) and Regulation P (12 C.F.R. Part 1016), may also govern the collection, use, or storage of biometric information.

Deception

- ***False or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information***

As with other types of technologies, false or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information constitute deceptive practices in violation of Section 5 of the FTC Act.[30] These claims can mislead both individual consumers and businesses that use these technologies. If prospective users rely on false or unsubstantiated claims in choosing one product over another, honest technology vendors who do not oversell their product's capabilities may be placed at a competitive disadvantage. Moreover, if business customers rely on these claims to use technologies that don't work as promised, they may ultimately harm consumers by, for instance, wrongly denying them benefits and opportunities. Thus, the Commission intends to carefully scrutinize claims about these technologies.

As with all marketing claims, the law requires that representations about biometric information technologies be substantiated when made—that is, persons or individuals making such claims must have a reasonable basis for their claims.[31] For example, businesses should be careful not to make false or unsubstantiated claims that technologies are unbiased. Claims of validity or accuracy are deceptive if they are true only for certain populations and if such limitations are not clearly stated.[32] Further, businesses must not make false or unsubstantiated claims about real-world validity, accuracy, or performance of biometric information technologies when the claims are based on tests or audits that do not replicate real-world conditions or how the technology will be operationalized by its intended users.[33] Businesses also should not make false or unsubstantiated claims that the technologies will deliver particular results or outcomes, such as reductions in rates of theft, violent incidents, fraud, or the elimination of bias in hiring.[34]

[30] *See* Complaint, *FTC v. Aura Labs, Inc.*, No. 8:16-cv-2147 (C.D. Cal. Dec. 2, 2016) (alleging company's representations that mobile application measured blood pressure with accuracy comparable to a traditional blood pressure cuff were false, misleading, or unsubstantiated); Complaint, *FTC v. New Consumer Solutions, LLC*, No. 1:15-cv-01614 (N.D. Il. Feb. 23, 2015) (alleging company's representations that a mobile application could detect melanoma by analyzing pictures of consumers' skin were false or unsubstantiated).

[31] *See, e.g.*, FTC Policy Statement Regarding Advertising Substantiation, appended to *In re Thompson Med. Co., Inc.,* 104 F.T.C. 648, 839 (1984), *aff'd,* 791 F.2d 189 (D.C. Cir. 1986). Where a company's claims of accuracy, efficacy, or lack of bias refer to specific facts or figures, they must generally be supported by a high level of substantiation, such as scientific or engineering tests. *See also Thompson Med.*, 104 F.T.C. at 822.

[32] *See, e.g.*, Complaint, *In re Everalbum*, FTC File No. 1923172 (May 6, 2021) (alleging company's representations that it was not using facial recognition unless user enabled it were deceptive, where the representations were true only for users in Texas, Illinois, Washington, and the European Union, and users outside of those locations were not provided a setting to turn off facial recognition); *In re J.B. Williams Co., Inc.*, 68 F.T.C. 481, 1965 WL 92965, *5 (1965), *aff'd*, 381 F.2d 884 (6th Cir. 1967) (claims that product could reduce fatigue were deceptive, where product was efficacious only in a small minority of cases where tiredness symptoms were due to an iron deficiency, and was of no benefit in all other cases).

[33] *See* Opinion of the Commission at 43-46, *In re ECM Biofilms, Inc.*, FTC File No. 1223118 (Oct. 19, 2015) (laboratory tests performed under aerobic conditions were not competent and reliable evidence of biodegradation in landfills, which are anaerobic environments), *aff'd*, 851 F.3d 599 (6th Cir. 2017).

[34] Claims that "significantly involve. . . safety," as well as claims relating to the performance or other central characteristics of a product or service, are generally material. FTC Policy Statement on Deception (Oct. 14, 1983), appended to *Cliffdale Associates, Inc.,* 103 F.T.C. 110, 174 (1984). *See also* Complaint, *In re Tapplock*, FTC File

- ***Deceptive statements about the collection and use of biometric information***

False or misleading statements about the collection and use of biometric information constitute deceptive acts in violation of Section 5 of the FTC Act, as does failing to disclose any material information needed to make a representation non-misleading. In recent years, the Commission has taken action against businesses that it charged with engaging in deceptive practices related to the collection and use of biometric information.[35] The Commission will continue to carefully scrutinize businesses' conduct in this area to ensure they are not misleading consumers. Businesses should not make false statements about the extent to which they collect or use biometric information or whether or how they implement technologies using biometric information.[36] Businesses also must ensure that they are not telling half-truths—for example, a business should not make an affirmative statement about some purposes for which it will use biometric information but fail to disclose other material uses of the information.[37]

<u>Unfairness</u>

The use of biometric information or biometric information technology may be an unfair practice within the meaning of the FTC Act. Under Section 5, a practice is unfair if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition.[38] As discussed above, the collection and use of biometric information can create a serious risk of harm to consumers. Such harms are not reasonably avoidable by consumers if the collection and use of such information is not clearly and conspicuously disclosed or if access to essential goods and services is conditioned on providing the information. For instance, if businesses automatically and surreptitiously collect consumers' biometric information as they enter or move through a store, the consumers have no ability to avoid the collection or use of that information.

Our past cases illustrate that collecting, retaining, or using consumers' personal information in ways that cause or are likely to cause substantial injury, or disseminating

No. 1923011 (May 18, 2020) (alleging that representations that smart padlock was secure were deceptive, where padlock had foreseeable information security vulnerabilities and could be quickly unlocked by unscrewing the back panel); Complaint, *FTC v. Lifelock, Inc.*, No. 2:10-cv-00530-MHM (D. Az. Mar. 8, 2010) (alleging that representations that service provided complete protection against all forms of identity theft were deceptive).

[35] *See* Complaint, *In re Everalbum*, FTC File No. 1923172 (May 6, 2021) (alleging that the company misrepresented that it was not using face recognition unless the user enabled it or turned it on); *See also* Complaint, *United States v. Facebook*, No. 19-cv-2184 (D.D.C. July 24, 2019) (alleging that the company misrepresented that users would have to "turn[ ] on" facial-recognition technology, violating a provision of a prior Commission order that prohibited misrepresenting the extent to which users could control the privacy of their data).

[36] *Id.*

[37] *See* Complaint, *United States v. Twitter*, No. 3:22-cv-03070 (N.D. Cal. May 25, 2022) (alleging that statements that users' telephone numbers provided for two-factor authentication would be used for security purposes were deceptive when the company failed to adequately disclose that such numbers would also be used for targeted advertising); Complaint, *In re Sears Holdings Mgmt. Corp.*, FTC File No. 082 3099 (Aug. 31, 2009) (alleging that respondents' statement that they would track consumers' "online browsing" was deceptive in light of failure to adequately disclose tracking of nearly all of the Internet behavior occurring on consumers' computers as well as certain non-Internet related activities taking place on those computers).

[38] 15 U.S.C. § 45(n); *see also* Letter from the FTC to Hon. Wendell Ford & Hon. John Danforth, Ranking Minority Member, S. Comm. on Com., Sci. & Transp., Consumer Subcomm., Comm'n Statement of Pol'y on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in In re Int'l Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984) (the "Unfairness Policy Statement").

technology that enables others to do so without taking reasonable measures to prevent harm to consumers can be an unfair practice in violation of Section 5 of the FTC Act.[39] For example, the FTC has previously charged that businesses have engaged in unfair practices by failing to protect consumers' personal information using reasonable data security practices; by engaging in invasive surveillance, tracking, or collection of sensitive personal information that was concealed from consumers or contrary to their expectations;[40] by, in certain circumstances, implementing privacy-invasive default settings;[41] by disseminating an inaccurate technology that, if relied on by consumers, could endanger them or others;[42] and by offering for sale technologies with the potential to cause or facilitate harmful and illegal conduct like covert tracking, and failing to take reasonable measures to prevent such conduct.[43] Additionally, the FTC has charged that certain discriminatory practices can be unfair.[44] Though many biometric information technologies are new, businesses must continue to abide by longstanding legal requirements and obligations.

In order to avoid liability under the FTC Act, businesses should implement reasonable privacy and data security measures to ensure that any biometric information that they collect or maintain is protected from unauthorized access—whether that access stems from an external

[39] *See generally, Privacy and Security*, FTC (last visited Mar. 29, 2023 11:28 AM), https://www.ftc.gov/business-guidance/privacy-security (collecting the FTC's published business guidance related to data privacy and security).

[40] *See, e.g.*, Complaint, *In re Lenovo, Inc.,* FTC File No. 1523134 3134 (Dec. 20, 2017) (alleging that preinstallation of ad-injecting software that, without adequate notice or informed consent, acted as a man-in-the-middle between consumers and all websites with which they communicated was unfair; and that failure to take reasonable measures to assess and address security risks created by the preinstalled software was unfair); Complaint, *FTC v. Vizio, Inc.* Case No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) (alleging that collection of sensitive television viewing activity without consent and contrary to consumer expectations, and sharing of such information with third parties, was an unfair practice); Complaint, *In re Showplace, Inc*., FTC File No. 1123151, (Apr. 11, 2013) (alleging that rent-to-own store's use of monitoring and tracking software installed on rented computers was an unfair practice).

[41] *See* Complaint, *United States v. Epic Games, Inc.*, Case No. 5:22-CV-00518 (E.D.N.C. Dec. 19, 2022) (alleging that developing and operating a ubiquitous, freely-available, and internet-enabled video game directed at children and teens that publicly broadcasted players' display names while putting children and teens in direct, real-time contact with others through on-by-default lines of voice and text communication (even after instituting an age gate on the service) was unfair); *see also*, Complaint, *FTC v. Frostwire LLC*, Case No. 111-cv-23643 (S.D. Fla. Oct. 11, 2011) (alleging that distributing an application with default settings that caused or were likely to cause consumers to unwittingly publicly share files already present on, or subsequently saved on, the consumers' mobile devices, including, among others, consumers' pictures, videos, and documents, was an unfair practice).

[42] *See* Complaint, *FTC v. Breathometer, Inc.*, No. 3:17-cv-314 (N.D. Cal. Jan. 23, 2017) (alleging that failing to notify consumers or take corrective action upon learning that device measuring blood alcohol levels was inaccurate was an unfair practice).

[43] *See, e.g.*, Complaint, *In re Support King*, *LLC*, FTC File No. 1923003 (Dec. 20, 2021) (alleging that the provider of software called "Spyfone," which allowed users to surreptitiously monitor and track others' devices, unfairly failed to take reasonable steps to ensure that the purchasers use the monitoring products and services only for legitimate and lawful purposes); Complaint, *In re Retina-X Studios, LLC*, FTC File No. 1723118 (Mar. 26, 2020) (alleging a failure to take reasonable steps to ensure that monitoring products and services that required circumventing certain security protections on mobile devices would be used only for legitimate and lawful purposes by the purchaser); Complaint, *In re DesignerWare, LLC*, FTC File No. 1123151 (Apr. 11, 2013) (alleging that furnishing rent-to-own stores with monitoring and tracking software to be installed on rented computers was an unfair practice).

[44] *See* Complaint, *FTC v. Passport Automotive Group*, Case. No. 8:22-cv-02670-GLS (D. Md. Oct. 18, 2022) (alleging that imposing higher costs on Black and Latino consumers than on similarly situated non-Latino White consumers was unfair); *see also* Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC: BUS. BLOG (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

cybersecurity intrusion or an internal incursion by unauthorized employees, contractors, or service providers.[45] Businesses must also take care that their own collection and use of biometric information is not likely to cause substantial consumer injury.

Determining whether a business's use of biometric information or biometric information technology violates Section 5 requires a holistic assessment of the business's relevant practices. In making such assessments, the Commission will draw on applicable lessons that can be derived from its past work—including, but not limited to, in privacy and data security matters. Importantly, in some situations, the adoption of a contemplated practice may be unjustifiable when weighing the potential risks to consumers against the anticipated benefits of the practice. For example, if more accurate, less risky alternatives are available, using a technology that is proven to have high error rates may present unjustifiable risk to consumers, even if the technology is more convenient, more efficient, or more profitable for the business considering implementing the technology. The Commission's assessment will take into account factors including, but not limited to, the following:

- ***Failing to assess foreseeable harms to consumers before collecting biometric information.***[46] Prior to collecting consumers' biometric information, or deploying a biometric information technology, businesses should conduct a holistic assessment of the potential risks to consumers associated with the collection and/or use.[47] For example, assessments should take into account the context in which the collection or use will take place and the extent to which the specific biometric information technologies to be used have been tested by the business or a third party.[48] The results of testing should be evaluated in light of how well the testing environment mirrors real world implementation and use, including the particular context in which the technology will be deployed. Assessments should also consider the role of human operators. Businesses should not conclude without evidence that the involvement of a human operator is sufficient to mitigate risks to consumers. Businesses should assess whether deploying a biometric information technology system leads to or contributes to outcomes that disproportionately harm particular demographics of consumers. These assessments should take into account

[45] Collecting or retaining biometric information without any legitimate business need or keeping that information indefinitely creates an increased risk of harm to consumers. *See, e.g.*, Complaint, *In re BJ's Wholesale Club, Inc.*, FTC File No. 0423160 (Sept. 20, 2005) (alleging a failure to employ reasonable and appropriate data security measures where, among other things, the company created unnecessary risks to sensitive financial information by storing it for up to 30 days when it no longer had a business need to keep the information); Complaint, *In re Residual Pumpkin Entity, LLC*, FTC File No. 1923209 (June 23, 2022) (alleging that company created unnecessary risks to personal information by storing it indefinitely on its network without a business need).

[46] *See, e.g.*, Complaint, *In re EPN, Inc.*, FTC File No. 1123143 (Oct. 3, 2012) (alleging a failure to assess risks to consumer personal information it collected and stored online.)

[47] *See, e.g.*, Complaint, *In re Lenovo, Inc.*, FTC File No. 1523134 (Dec. 20, 2017) (alleging that respondent's failure to take reasonable measures to assess and address security risks created by third-party software it installed on laptops it offered to consumers was an unfair practice); Complaint, *In re SettlementOne Credit Corp.*, FTC File No. 0823208 (Aug. 17, 2011) (alleging that respondents failed to assess the risks of allowing end users with unverified or inadequate security to access consumer reports through respondents' portal).

[48] *See, e.g.*, Complaint, *In re Upromise, Inc.*, FTC File No. 1023116 (Mar. 27, 2012) (alleging unfair conduct, where defendant allegedly engaged a service provider to develop software that it distributed to consumers but failed, among other things, to assess and address risks posed by the software by testing, post-deployment monitoring, or other means).

whether technical components of the system, such as algorithms, have been specifically tested for differential performance across demographic groups—including intersectionally.

- ***Failing to promptly address known or foreseeable risks,***[49] including by failing to identify and implement readily available tools for reducing or eliminating risks.[50] For instance, if there is evidence that a particular biometric information technology is often prone to certain types of errors or biases, businesses should proactively take appropriate measures to reduce or eliminate the risk that such errors could lead to consumer injury. Steps taken to address risks may include organizational measures, such as policies and procedures to appropriately limit access to biometric information.[51] They may also include technical measures. For example, businesses should timely update relevant systems, including both software components like algorithms and hardware components that are used to capture, process, or store biometric information, in order to ensure that the systems operate effectively and do not put consumers at risk.[52]

- ***Engaging in surreptitious and unexpected collection or use of biometric information.*** [53] In some situations, such conduct may be unfair in and of itself. For instance, businesses may violate the law if they use or facilitate the use of biometric information or biometric information technology to surreptitiously identify or track a consumer in a manner that exposes the consumer to risks such as stalking, exposure to stigma, reputational harm, or

[49] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602, 624-26 (D.N.J. Apr. 7, 2014) (holding that the FTC's complaint adequately stated a claim for unfair data security practices where it alleged, among other things, defendant permitted its hotels to connect insecure servers to its network, including servers with outdated operating systems that could not receive patches to address known security vulnerabilities), *aff'd*, 799 F.3d 236 (3d Cir. 2015); Complaint, *FTC v. Equifax, Inc.*, No. 1:19-cv-03297-TWT (N.D. Ga. July 22, 2019) (alleging failure to implement reasonable procedures to detect, respond to, and timely correct critical and other high-risk security vulnerabilities across Defendant's systems); Complaint, *In re Lookout Services, Inc.*, FTC File No. 1023076 (June 15, 2011) (alleging respondent's failure to adequately assess or address the vulnerability of its web application to widely-known security flaws).

[50] *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC*, FTC File No. 1923209 (June 23, 2022) (alleging a failure to implement readily available protections against well-known and reasonably foreseeable vulnerabilities); Complaint, *In re Compete, Inc.*, FTC File No. 1023155 (Feb. 20, 2013) (alleging a failure to use readily available, low-cost measures to assess/address the risk that data collection software would collect sensitive consumer information it was not authorized to collect).

[51] *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC*, FTC File No. 1923209 (June 23, 2022) (alleging that Residual Pumpkin failed to establish or enforce rules sufficient to make user credentials hard to guess and failed to implement patch management policies and procedures to ensure the timely remediation of critical security vulnerabilities and use of obsolete versions of database and web server software that no longer received patches); Complaint, *FTC v. Equifax, Inc.*, No. 1:19-cv-03297-TWT (N.D. Ga. July 22, 2019) (alleging failure to implement or enforce reasonable access controls to prevent unauthorized access to sensitive personal information).

[52] *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC*, FTC File No. 1923209 (June 23, 2022) (alleging failure to implement patch management policies and procedures to ensure the timely remediation of critical security vulnerabilities and use of obsolete versions of database and web server software that no longer received patches).

[53] *See, e.g.*, Complaint, *In re Aaron's, Inc.*, FTC File No. 1223264 (Mar. 10, 2014) (alleging that allowing franchisees to install software facilitating surreptitious collection of private information on rented computers was an unfair practice, and noting that consumers were unable to avoid harm because collection was surreptitious).

extreme emotional distress.[54] Additionally, as discussed above, failing to clearly and conspicuously disclose the collection and use of biometric information makes such collection and use unavoidable by the consumer. Injuries to consumers may also be compounded if there is no mechanism for accepting and addressing consumer complaints and disputes related to businesses' use of biometric information technologies.

- ***Failing to evaluate the practices and capabilities of third parties,*** including affiliates, vendors, and end users, who will be given access to consumers' biometric information or will be charged with operating biometric information technologies. Businesses should seek relevant assurances and contractual agreements that require third parties to take appropriate steps to minimize risks to consumers. They should also go beyond contractual measures to oversee third parties and ensure they are meeting those requirements and not putting consumers at risk.[55] Such oversight may include organizational and technical measures (including taking steps to ensure access to necessary information) to supervise, monitor or audit the third parties' compliance with any requirements.

- ***Failing to provide appropriate training for employees and contractors*** whose job duties involve interacting with biometric information or technologies that use such information.[56]

[54] *See, e.g.*, Complaint, *In re Support King*, FTC File No. 1923003 (Dec. 20, 2021) (alleging that respondents' SpyFone monitoring products and services substantially injure device users by enabling purchasers to stalk them surreptitiously); Complaint, *In re Retina-X Studios, LLC*, FTC File No. 1723118 (Mar. 26, 2020) (similarly alleging respondent's products and services substantially injure device users by enabling purchasers to surreptitiously stalk them); Complaint, *FTC v. EMP Media, Inc.*, No. 2:18-cv-00035 (D. Nev. Jan. 9, 2018) (alleging that defendants published consumers' intimate images without consent in a manner enabling the public to identify or contact the individuals depicted, causing a number of harms to consumers including an unwarranted invasion of privacy into consumers' lives, depression, anxiety, loss of reputation, safety fears, medical and legal costs, and lost time, was unfair)).

[55] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 241 (3d Cir. 2015) (affirming denial of motion to dismiss FTC's complaint alleging unfair data security practices, which included allegations defendant allowed hotel property management systems to connect to its network without taking appropriate precautions, such as ensuring that the hotels implemented adequate information security policies and procedures); Complaint, *In re GeneLink, Inc.*, FTC File No. 1123095 (May 8, 2014) (alleging that company unfairly failed to employ reasonable and appropriate measures to prevent unauthorized access to consumers' personal information because, among other things, it failed to provide reasonable oversight of service providers); *See, e.g.*, Complaint, *In re Upromise, Inc*., FTC File No. 1023116 (Mar. 27, 2012) (alleging failure to take adequate measures to ensure that its service provider employed reasonable and appropriate measures to protect consumer information and to implement the information collection program in a manner consistent with contractual provisions designed to protect consumer information).

[56] *See, e.g.*, Complaint, *In re SkyMed Int'l , Inc*., FTC File No. 1923140 (Jan. 26, 2021) (alleging a failure to provide adequate guidance or training for employees or third-party contractors regarding information security and safeguarding consumers' personal information); Complaint, *In re Zoom Video Communc'ns, Inc.*, FTC File No. 1923167 (Jan. 19, 2021) (alleging that failure to implement a training program on secure software development principles contributed to unfair conduct).

- ***Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale,[57] or uses[58] in connection with biometric information*** to ensure that the technologies are functioning as anticipated, that users of the technology are operating it as intended, and that use of the technology is not likely to harm consumers.

The Commission notes that a practice need not be equally likely to harm all consumers in order to be considered unfair. In determining what constitutes reasonable practices to protect consumers from potential harms associated with the use of biometric information, therefore, the Commission will—and businesses should—consider the practices from the perspective of any population of consumers that is particularly at risk of those harms.[59]

Finally, the Commission wishes to emphasize that—particularly in view of rapid changes in technological capabilities and uses—businesses should continually assess whether their use of biometric information or biometric information technologies causes or is likely to cause consumer injury in a manner that violates Section 5 of the FTC Act. If so, businesses must cease such practices, whether or not the practices are specifically addressed in this statement.

[57] *See, e.g.*, Complaint, *In re ASUSTeK Computer Inc.*, FTC File No. 1423156 (July 18, 2016) (alleging a failure to perform vulnerability and penetration testing on software that respondent offered for sale, including for well-known and reasonably foreseeable vulnerabilities that could be exploited to gain unauthorized access to consumers' sensitive personal information and local networks).

[58] *See, e.g.*, Complaint, *FTC v. Equifax, Inc.*, No. 1:19-cv-03297-TWT (N.D. Ga. July 22, 2019) (alleging failure to implement reasonable procedures to detect, respond to, and timely correct critical and other high-risk security vulnerabilities across Defendant's systems); Complaint, *In re SettlementOne Credit Corp.*, FTC File No. 0823208 (Aug. 19, 2011) (alleging that respondents failed to implement reasonable steps to maintain an effective system of monitoring access to consumer reports by end users).

[59] *See, e.g.*, Unfairness Policy Statement, *supra* n. 36, at 1074 ("[S]ome may exercise undue influence over highly susceptible classes of purchasers, as by promoting fraudulent 'cures' to seriously ill cancer patients."); Complaint, *In re Philip Morris, Inc.*, 82 F.T.C. 16 (1973) (alleging respondent engaged in an "unfair and deceptive act and practice" by distributing free-sample razor blades in home-delivered newspapers, which posed a particular hazard to young children).

Press release

09-12-2023 - 00:04
20231206IPR15699

European Parliament

Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI

- Safeguards agreed on general purpose artificial intelligence
- Limitation for the of use biometric identification systems by law enforcement
- Bans on social scoring and AI used to manipulate or exploit user vulnerabilities
- Right of consumers to launch complaints and receive meaningful explanations
- Fines ranging from 35 million euro or 7% of global turnover to 7.5 million or 1.5% of turnover

MEPs reached a political deal with the Council on a bill to ensure AI in Europe is safe, respects fundamental rights and democracy, while businesses can thrive and expand.

On Friday, Parliament and Council negotiators reached a provisional agreement on the Artificial Intelligence Act. This regulation aims to ensure that fundamental rights, democracy, the rule of law and environmental sustainability are protected from high risk AI, while boosting innovation and making Europe a leader in the field. The rules establish obligations for AI based on its potential risks and level of impact.

Banned applications

Recognising the potential threat to citizens' rights and democracy posed by certain applications of AI, the co-legislators agreed to prohibit:

- biometric categorisation systems that use sensitive characteristics (e.g. political, religious, philosophical beliefs, sexual orientation, race);
- untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases;
- emotion recognition in the workplace and educational institutions;
- social scoring based on social behaviour or personal characteristics;
- AI systems that manipulate human behaviour to circumvent their free will;
- AI used to exploit the vulnerabilities of people (due to their age, disability, social or economic situation).

Law enforcement exemptions

Negotiators agreed on a series of safeguards and narrow exceptions for the use of biometric identification systems (RBI) in publicly accessible spaces for law enforcement purposes, subject to prior judicial authorisation and for strictly defined lists of crime. “Post-remote” RBI would be used strictly in the targeted search of a person convicted or suspected of having committed a serious crime.

“Real-time” RBI would comply with strict conditions and its use would be limited in time and location, for the purposes of:

- targeted searches of victims (abduction, trafficking, sexual exploitation),
- prevention of a specific and present terrorist threat, or
- the localisation or identification of a person suspected of having committed one of the specific crimes mentioned in the regulation (e.g. terrorism, trafficking, sexual exploitation, murder, kidnapping, rape, armed robbery, participation in a criminal organisation, environmental crime).

Obligations for high-risk systems

For AI systems classified as high-risk (due to their significant potential harm to health, safety, fundamental rights, environment, democracy and the rule of law), clear obligations were agreed. MEPs successfully managed to include a mandatory fundamental rights impact assessment, among other requirements, applicable also to the insurance and banking sectors. AI systems used to influence the outcome of elections and voter behaviour, are also classified as high-risk. Citizens will have a right to launch complaints about AI systems and receive explanations about decisions based on high-risk AI systems that impact their rights.

Guardrails for general artificial intelligence systems

To account for the wide range of tasks AI systems can accomplish and the quick expansion of its capabilities, it was agreed that general-purpose AI (GPAI) systems, and the GPAI models they are based on, will have to adhere to transparency requirements as initially proposed by

Parliament. These include drawing up technical documentation, complying with EU copyright law and disseminating detailed summaries about the content used for training.

For high-impact GPAI models with systemic risk, Parliament negotiators managed to secure more stringent obligations. If these models meet certain criteria they will have to conduct model evaluations, assess and mitigate systemic risks, conduct adversarial testing, report to the Commission on serious incidents, ensure cybersecurity and report on their energy efficiency. MEPs also insisted that, until harmonised EU standards are published, GPAIs with systemic risk may rely on codes of practice to comply with the regulation.

Measures to support innovation and SMEs

MEPs wanted to ensure that businesses, especially SMEs, can develop AI solutions without undue pressure from industry giants controlling the value chain. To this end, the agreement promotes so-called regulatory sandboxes and real-world-testing, established by national authorities to develop and train innovative AI before placement on the market.

Sanctions and entry into force

Non-compliance with the rules can lead to fines ranging from 35 million euro or 7% of global turnover to 7.5 million or 1.5 % of turnover, depending on the infringement and size of the company.

Quotes

Following the deal, co-rapporteur Brando Benifei (S&D, Italy) said: “It was long and intense, but the effort was worth it. Thanks to the European Parliament’s resilience, the world’s first horizontal legislation on artificial intelligence will keep the European promise - ensuring that rights and freedoms are at the centre of the development of this ground-breaking technology. Correct implementation will be key - the Parliament will continue to keep a close eye, to ensure support for new business ideas with sandboxes, and effective rules for the most powerful models”.

Co-rapporteur Dragos Tudorache (Renew, Romania) said: “The EU is the first in the world to set in place robust regulation on AI, guiding its development and evolution in a human-centric direction. The AI Act sets rules for large, powerful AI models, ensuring they do not present systemic risks to the Union and offers strong safeguards for our citizens and our democracies against any abuses of technology by public authorities. It protects our SMEs, strengthens our capacity to innovate and lead in the field of AI, and protects vulnerable sectors of our economy.

The European Union has made impressive contributions to the world; the AI Act is another one that will significantly impact our digital future”.

Press conference

Lead MEPs Brando Benifei (S&D, Italy) and Dragos Tudorache (Renew, Romania), the Secretary of State for digitalisation and artificial intelligence Carme Artigas, and Commissioner Thierry Breton held a joint press conference after the negotiations. You can re-watch the statement of Mr Benifei and the statement of Mr Tudorache, and see more extracts from the press conference.

Next steps

The agreed text will now have to be formally adopted by both Parliament and Council to become EU law. Parliament’s Internal Market and Civil Liberties committees will vote on the agreement in a forthcoming meeting.

Further information

Committee on the Internal Market and Consumer Protection
Committee on Civil Liberties, Justice and Home Affairs

Contacts

Yasmina YAKIMOVA
Press Officer
☎ (+32) 2 28 42626 (BXL)
📱 (+32) 470 88 10 60
✉ yasmina.yakimova@europarl.europa.eu

Janne OJAMO
Press Officer
☎ (+32) 2 284 12 50 (BXL)
📱 (+32) 470 89 21 92
✉ janne.ojamo@europarl.europa.eu

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

DRAFT
AUTOMATED DECISIONMAKING TECHNOLOGY REGULATIONS

DECEMBER 2023

Statutory Provisions for Reference:

Delegation of rulemaking authority to the California Privacy Protection Agency as set forth in Civil Code section 1798.185, subdivision (a)(16):

> Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

[ADDITIONS TO] § 7001. Definitions.

"Automated decisionmaking technology" means any system, software, or process—including one derived from machine-learning, statistics, or other data-processing or artificial intelligence—that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decisionmaking. Automated decisionmaking technology includes profiling.

"Decision that produces legal or similarly significant effects concerning a consumer" means a decision that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services.

"Profiling" means any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Publicly accessible place" means a place that is open to or serves the public. Examples of publicly accessible places include shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums, hospitals, medical clinics or offices, transportation depots, transit, streets, or parks.

[ADDITION] § 7017. Notice of Rights to Opt-Out of, and Access Information About, the Business's Use of Automated Decisionmaking Technology.

(a) A business that uses automated decisionmaking technology as set forth in sections 7030, subsection (b), and 7031, subsection (b), shall provide consumers with the Notice of Rights to Opt-Out of, and Access Information About, the Business's Use of Automated Decisionmaking Technology ("Pre-use Notice"). The Pre-use Notice shall inform consumers about the business's use of automated decisionmaking technology and consumers' rights to opt-out of, and to access information about, the business's use of automated decisionmaking technology.

(b) The Pre-use Notice shall:

(1) Comply with section 7003;

(2) Be made readily available where consumers will encounter it;

(3) Be provided in the manner in which the business primarily interacts with the consumer, before the business processes the consumer's personal information using the automated decisionmaking technology; and

(4) Include the following:

(A) A plain language explanation of the purpose for which the business proposes to use the automated decisionmaking technology. The purpose shall not be described in generic terms, such as "to improve our services," because generic terms are insufficient for the consumer to understand the business's proposed purpose for using the automated decisionmaking technology.

(B) A description of the consumer's right to opt-out of the business's use of the automated decisionmaking technology for the processing activities set forth in section 7030, subsection (b), and how the consumer can submit a request to opt-out of the business's use of the automated decisionmaking technology. This description of the consumer's right to opt-out shall clearly state the scope of their opt-out right.

(i) If the business is not required to provide a right to opt-out because it is relying upon an exception in section 7030, subsection (m), it shall inform the consumer of that fact and identify the specific exception it is relying upon.

(C) A description of the consumer's right to access information about the business's use of the automated decisionmaking technology with respect to the consumer for the processing activities set forth in section 7031, subsection (b), and how the consumer can submit their access request.

(D) A simple and easy-to-use method (e.g., a layered notice or hyperlink) by which the consumer can obtain additional information about the business's use of the automated decisionmaking technology.

(i) This additional information shall include a plain language explanation of the following:

1. The logic used in the automated decisionmaking technology, including the key parameters that affect the output of the automated decisionmaking technology. The business shall explain why these parameters are key;

2. The intended output of the automated decisionmaking technology (e.g., a numerical score of compatibility);

3. How the business plans to use the output to make a decision, including the role of any human involvement; and

4. Whether the business's use of the automated decisionmaking technology has been evaluated for validity, reliability, and fairness, and the outcome of any such evaluation.

(ii) The business also may include in the Pre-use Notice a hyperlink that directs the consumer to its unabridged risk assessment for the business's use of the automated decisionmaking technology.

(c) If a business is using automated decisionmaking technology as set forth in section 7030, subsection (m), the business shall not be required to notify consumers about the right to opt-out of the processing in a Pre-use Notice for that use.

(d) If a business is using automated decisionmaking technology as set forth in section 7030, subsections (m)(1)–(3), the business shall not be required to disclose information in a Pre-use Notice that would compromise its processing of personal information for those purposes.

[ADDITION] § 7030. Requests to Opt-Out of the Business's Use of Automated Decisionmaking Technology.

(a) Consumers have a right to opt-out of businesses' use of automated decisionmaking technology as set forth in this section.

(b) A business shall provide consumers with the ability to opt-out of the following uses of automated decisionmaking technology:

(1) For a decision that produces legal or similarly significant effects concerning a consumer;

(2) Profiling a consumer who is acting in their capacity as an employee, independent contractor, job applicant, or student. For example, this includes profiling an employee using keystroke loggers, productivity or attention monitors, video or audio recording or live-streaming, facial- or speech-recognition or -detection, automated emotion assessment, location trackers, speed trackers, and web-browsing, mobile-application, or social-media monitoring tools;

(3) Profiling a consumer while they are in a publicly accessible place. For example, this includes profiling a consumer while they are in a publicly accessible place using wi-fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live-streaming, facial- or speech- recognition or -detection, automated emotion assessment, geofencing, location trackers, or license-plate recognition;

(4) **SUBCOMMITTEE OPTION FOR BOARD DISCUSSION:** Profiling a consumer for behavioral advertising;

(A) A business that profiles a consumer that the business has actual knowledge is under the age of 16 for behavioral advertising shall comply with the requirements set forth in sections 7070 and 7071;

ADDITIONAL OPTIONS FOR BOARD DISCUSSION

(5) Profiling a consumer that the business has actual knowledge is under the age of 16; or

(6) Processing the personal information of consumers to train automated decisionmaking technology.

(c) A business that uses automated decisionmaking technology as set forth in subsection (b) shall provide two or more designated methods for submitting requests to opt-out of the business's use of the automated decisionmaking technology. A business shall consider the methods by which it interacts with consumers, the manner in which the business uses the automated decisionmaking technology, and the ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of the business's use of the automated decisionmaking technology. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples and requirements follow.

(1) A business that interacts with consumers online shall, at a minimum, allow consumers to submit requests to opt-out through an interactive form accessible via an opt-out link that is provided in the Pre-use Notice. The link shall be titled [*Note: Agency staff recommends receiving public comment on what the link(s) should be titled for consumers to understand the scope of the opt-out right*].

(2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out in addition to the online form.

(3) Other methods for submitting requests to opt-out include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of the business's use of automated decisionmaking technology because cookies concern the collection of personal information and not necessarily the use of automated decisionmaking technology. An acceptable method for submitting requests to opt-out must be specific to the right to opt-out of the business's use of the automated decisionmaking technology.

(d) A business's methods for submitting requests to opt-out of the business's use of the automated decisionmaking technology shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

(e) A business shall not require a consumer submitting a request to opt-out of the business's use of the automated decisionmaking technology to create an account or provide additional information beyond what is necessary to direct the business to opt-out the consumer.

(f) Except as set forth in subsection (f)(1), a business may require a verified consumer request if it has determined and documented that consumers are more likely than not to be negatively impacted if the business were to honor a fraudulent request to opt-out consumers of the business's use of the automated decisionmaking technology. Negative impacts are those set forth in section 7152, subsection (a)(8). If a business determines that verification is necessary, it shall comply with the requirements for verification in Article 5.

(1) A business shall not require a verifiable consumer request for a request to opt-out of profiling for behavioral advertising. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information is subject to the business's profiling for behavioral advertising. However, to the extent that the business can comply with a request to opt-out without additional information, it shall do so.

(g) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of the business's use of automated decisionmaking technology is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

(h) If the consumer submits a request to opt-out of the business's use of automated decisionmaking technology as set forth in subsection (b), before the business has initiated that processing, the business shall not initiate processing of the consumer's personal information using that automated decisionmaking technology. If the consumer did not opt-out in response to the Pre-use Notice, and submitted a request to opt-out after the business initiated the processing, the business shall comply with the consumer's opt-out request by:

(A) Ceasing to process the consumer's personal information using that automated decisionmaking technology as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. For personal information previously processed by that automated decisionmaking technology, the business shall neither use nor retain that information; and

(B) Notifying all the business's service providers, contractors, or other persons to whom the business has disclosed or made personal information available to process the consumer’s personal information using that automated decisionmaking technology, that the consumer has made a request to opt-out, and instructing them to comply with the consumer’s request to opt-out of the business’s use of that automated decisionmaking technology within the same time frame.

(i) A business shall provide a means by which the consumer can confirm that the business has processed their request to opt-out of the business’s use of the automated decisionmaking technology.

(j) In responding to a request to opt-out of the business’s use of automated decisionmaking technology, a business may present the consumer with the choice to allow specific uses of automated decisionmaking technology as long as a single option to opt-out of all of the business’s uses of automated decisionmaking technology set forth in subsection (b) is also offered.

(k) A consumer may use an authorized agent to submit a request to opt-out of the business’s use of the automated decisionmaking technology on the consumer’s behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer’s signed permission demonstrating that they have been authorized by the consumer to act on the consumer’s behalf.

(l) Except as allowed by these regulations, a business shall wait at least 12 months from the date the business receives the consumer’s request to opt-out of the business’s use of the automated decisionmaking technology before asking a consumer who has exercised their right to opt-out, to consent to the business’s use of the automated decisionmaking technology for which the consumer previously opted out.

(m) A business is not required to provide consumers with the ability to opt-out of the use of automated decisionmaking technology if the business’s use of that automated decisionmaking technology is compliant with section 7002, and the business’s use of that automated decisionmaking technology is necessary to achieve, and is used solely for, the following purposes:

(1) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;

(2) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions;

(3) To protect the life and physical safety of consumers; or

(4) To provide the good or perform the service specifically requested by the consumer.

(A) If a business's use of the automated decisionmaking technology is to provide a good or opportunity or perform a service as set forth in subsection (m)(4), the business also must have no reasonable alternative method of processing as set forth below.

(B) There is a rebuttable presumption that the business has a reasonable alternative method of processing if there is an alternative method of processing that is or has been used in the business's industry or similar industries to provide a similar good or perform a similar service.

(C) The business may rebut this presumption by demonstrating one or more of the following factors:

(i) It would be futile for the business to develop or use alternative methods of processing. For example, if a business provides resume-screening and job-matching services and must screen thousands of resumes to recommend job-matches for a same-day job opportunity, the business could demonstrate the futility of developing or using a non-automated decisionmaking process because it would be futile to use a non-automated decisionmaking process to screen thousands of resumes within a few hours;

(ii) Developing and using an alternative method of processing would result in a good or service that is not as valid, reliable, and fair. For example, if the business offers a resume-screening and job-matching service, and an alternative method of processing for identifying qualified job applicants is more likely than the automated decisionmaking technology to have a disparate impact on protected classes, then using that alternative method of processing would result in a service that is not as fair; or

(iii) Developing an alternative method of processing would impose extreme hardship upon the business, considering the business's overall financial resources and the nature and structure of its operation, including the business's technical capabilities. For example, for a business with $25 million in annual gross revenue and 20 employees, if the only available alternative method of processing would impose a multi-million-dollar expense or require the business to hire 50 new employees with specific technical expertise, the business could demonstrate that developing this alternative method of processing would impose extreme hardship upon the business.

(D) If there is no alternative method of processing that is or has been used in the business's industry or similar industries to provide a similar good or perform a similar service, and the business can demonstrate any of the factors set forth in subsections (C)(i)–(iii), the business has no reasonable alternative method of processing.

(E) Any business relying on this exception to not provide a consumer with the ability to opt-out of its use of the automated decisionmaking technology shall document its explanation of how it meets the requirements in subsection (m)(4)(A)–(D), and shall provide such explanation to the Agency within five (5) business days of the Agency's request.

(n) If a business is profiling a consumer for behavioral advertising, the business cannot rely on the exceptions set forth in subsection (m) and shall be required to provide consumers with the ability to opt-out of that use of automated decisionmaking technology.

(o) If a business is using automated decisionmaking technology as set forth in subsection (b), the business shall provide consumers with a method to submit a complaint about the business's use of the automated decisionmaking technology to the business, and shall explain how consumers can submit a complaint.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

[ADDITION] § 7031. Requests to Access Information About the Business's Use of Automated Decisionmaking Technology.

(a) Consumers have a right to access information about the business's use of automated decisionmaking technology as set forth in this section.

(b) If the business uses automated decisionmaking technology for any processing set forth in section 7030, subsection (b), then the business shall provide consumers with access to information about the business's use of that automated decisionmaking technology ("right to access" or "access right").

(c) A business's methods for consumers to submit requests to exercise their access right shall comply with section 7020.

(d) If a business has made a decision that results in the denial of goods or services as set forth in section 7030, subsection (b)(1), with respect to the consumer (e.g., denied the consumer an employment opportunity or lowered their compensation), the business shall notify the consumer of the following, via the method by which the business primarily interacts with the consumer:

(1) That the business made a decision with respect to the consumer;

(2) That the consumer has a right to access information about the business's use of that automated decisionmaking technology;

(3) How the consumer can exercise their access right; and

(4) That the consumer can file a complaint with the Agency and the Attorney General. The business also shall provide links to the complaint forms on their respective websites. For example, the business can include the following language in its response to the consumer: "If you believe your privacy rights have been violated, you can submit a complaint to the California Privacy Protection Agency at [link to complaint form] or to the California Attorney General at [link to complaint form]."

(e) For requests to exercise the right to access, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business shall not disclose the information identified in subsections (i)(2)–(5) and shall inform the requestor that it cannot verify their identity.

(f) If a business denies a consumer's verified request to exercise their right to access, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.

(g) A business shall use reasonable security measures when transmitting the requested information to the consumer.

(h) If a business maintains a password-protected account with the consumer, it may comply with a request to exercise the right to access by using a secure self-service portal for consumers to access, view, and receive a portable copy of their requested information if the portal fully discloses the requested information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.

(i) In responding to a consumer's request to exercise their access right, a business shall provide plain language explanations of the following information to the consumer:

(1) The purpose for which the business used automated decisionmaking technology. The purpose shall not be described in generic terms, as set forth in section 7017, subsection (b)(4)(A).

(2) The output of the automated decisionmaking technology with respect to the consumer.

(A) If the business has multiple outputs with respect to the consumer, the business shall provide a simple and easy-to-use method by which the consumer can access all of the outputs.

(3) How the business used the output to make a decision with respect to the consumer. This explanation shall include:

(A) The decision (including, for example, the placement of a consumer into a category or segment as a result of profiling) that was made, executed, or facilitated by the business's use of the automated decisionmaking technology with respect to the consumer;

(B) Any factors other than the output that the business used to make the decision;

(C) The role of any human involvement in the business's use of the automated decisionmaking technology; and

(D) Whether the business's use of the automated decisionmaking technology has been evaluated for validity, reliability, and fairness, and the outcome of any such evaluation.

(4) If the business plans to use the output to make a decision with respect to the consumer, the business's explanation shall include:

(A) How the business plans to use the output to make a decision with respect to the consumer;

(B) Any factors other than the output that the business plans to use to make the decision;

(C) The role of any human involvement in the business's use of the automated decisionmaking technology; and

(D) Whether the business's use of the automated decisionmaking technology has been evaluated for validity, reliability, and fairness, and the outcome of any such evaluation.

(5) How the automated decisionmaking technology worked with respect to the consumer. At a minimum, this explanation shall include:

(A) How the logic, including its assumptions and limitations, was applied to the consumer; and

(B) The key parameters that affected the output of the automated decisionmaking technology. The business shall explain why the parameters were key, and how those parameters applied to the consumer.

(6) A simple and easy-to-use method by which the consumer can obtain the range of possible outputs, which may include aggregate output statistics (for example, the five most common outputs of the automated decisionmaking technology, on average, across all consumers during the preceding

calendar year, and the percentage of consumers that received each output during the preceding calendar year).

(7) Instructions for how the consumer can exercise their other CCPA rights. These instructions shall include any links to an online request form or portal for making such a request, if offered by the business.

(A) The business may comply with this requirement by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains these instructions. Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain these instructions, so that the consumer is required to scroll through other information in order to find the instructions, does not satisfy this standard.

(8) In accordance with the requirement in section 7030, subsection (o), the business shall provide instructions regarding the method by which the consumer can submit a complaint to the business about the business's use of the automated decisionmaking technology, including a complaint about a specific decision and how the decision was or will be made with respect to the consumer. The business also shall:

(A) Explain that the consumer can file a complaint with the Agency and the Attorney General and provide links to the complaint forms on their respective websites. For example, the business can include the following language in its response to the consumer: "If you believe your privacy rights have been violated, you can submit a complaint to the California Privacy Protection Agency at [link to complaint form] or to the California Attorney General at [link to complaint form]."

(j) If a business's use of the automated decisionmaking technology is solely as set forth in section 7030, subsection (m), the business shall not be required to provide the ability to opt-out or an opt-out link or include information about this right in its response to a request to access.

(k) If a business's use of the automated decisionmaking technology is solely as set forth in section 7030, subsections (m)(1)–(3), the business shall not be required to disclose information in its response to a request to access that would compromise its processing of personal information for those purposes.

(l) A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to access, including by providing the business with the consumer's personal information it has in its possession that it collected pursuant to their written contract with the business, or by enabling the business to access that personal information.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

For Consideration in Conjunction with Section 7030, Subsection (b)(4)(A) ("Profiling for Behavioral Advertising")

[ADDITIONS TO] ARTICLE 6. SPECIAL RULES REGARDING CONSUMERS UNDER 16 YEARS OF AGE

§ 7070. Consumers Less Than 13 Years of Age.

(c) Process for Opting-In to Profiling for Behavioral Advertising

(1) A business that has actual knowledge that it profiles a consumer less than the age of 13 for behavioral advertising shall establish, document, and comply with a reasonable method for a parent or guardian of that child to opt-in to the use of profiling for behavioral advertising, and for determining that the person consenting to the profiling is the parent or guardian of that child. This consent to the profiling is in addition to any verifiable parental consent required under COPPA.

(2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include those set forth in subsection (a)(2).

(d) When a business receives consent to profiling for behavioral advertising pursuant to subsection (c), the business shall inform the parent or guardian of the right to opt-out of profiling for behavioral advertising and of the process for doing so on behalf of their child pursuant to section 7030.

§ 7071. Consumers at Least 13 Years of Age and Less Than 16 Years of Age.

(c) A business that has actual knowledge that it profiles a consumer at least 13 years of age and less than 16 years of age for behavioral advertising shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the use of profiling for behavioral advertising.

(d) When a business receives a request to opt-in to the profiling of a consumer at least 13 years of age and less than 16 years of age for behavioral advertising, the business shall inform the consumer of their ongoing right to opt-out of the use of profiling for behavioral advertising at any point in the future and of the process for doing so pursuant to section 7030.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION,

Plaintiff,

-vs-

Case No.: 1:22-cv-2565--PKC-PK

ITUTORGROUP, INC.; TUTOR GROUP LIMITED; and
SHANGHAI PING'AN INTELLIGENT EDUCATION
TECHNOLOGY CO. LTD.,

Defendants.

JOINT NOTICE OF SETTLEMENT AND REQUEST FOR APPROVAL AND EXECUTION OF CONSENT DECREE

The parties in this matter have reached a settlement pursuant to the terms of the attached Consent Decree. In accordance with the terms of the Consent Decree, the Court will retain jurisdiction over this action for all purposes including the entering of all necessary orders, judgments, and decrees.

The Parties jointly request that the Court approve and execute the attached Consent Decree. Pursuant to the terms of the Consent Decree, upon signature and approval by the Court, the matter will be administratively closed but not dismissed.

Dated: August 09, 2023

By: DANIEL SELTZER
Daniel Seltzer
EEOC
33 Whitehall Street
5th Floor
New York, New York 10004-2112
929-506-5308
daniel.seltzer@eeoc.gov

Attorney for Plaintiff

By: ________________________
Michael J Sheppeard
SCARINCI HOLLENBECK LLC
589 8th Avenue
16th Fl
New York, NY 10018
P: 212.286.0747
msheppeard@sh-law.com

Attorney for All Defendants

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION,

Plaintiff,

-vs-

ITUTORGROUP, INC.; TUTOR GROUP LIMITED; and SHANGHAI PING'AN INTELLIGENT EDUCATION TECHNOLOGY CO. LTD.,

Defendants.

Case No.: 1:22-cv-2565--PKC-PK

CONSENT DECREE

WHEREAS, on May 5, 2022, the EEOC brought this Lawsuit under the Age Discrimination in Employment Act (the "ADEA") alleging unlawful employment practices on the basis of age and seeking to provide appropriate relief to Charging Party Wendy Pincus and a class of similarly aggrieved individuals who were allegedly denied employment as tutors because of their age.

WHEREAS, the EEOC specifically alleged that: (i) Defendants iTutorGroup, Inc. ("iTutorUSA"), Shanghai Ping'An Intelligent Education Technology Co., Ltd. ("Shanghai Ping"), and Tutor Group Limited ("Tutor Group") (iTutorUSA, Shanghai Ping, and Tutor Group will be collectively referred to as "Defendants") were providers of English-language tutoring services to students in China under the "iTutorGroup" brand name; (ii) Defendants programmed their application software to automatically reject female applicants over the age of 55 and male applicants over the age of 60; and (iii) in early 2020, Defendants failed to hire Charging Party Wendy Pincus and more than 200 other qualified applicants age 55 and older from the United States because of their age.

WHEREAS, Defendants filed an Answer to the Complaint denying the EEOC's allegations in their entirety and asserted numerous affirmative defenses.

WHEREAS, Defendants have denied and continue to deny all of the allegations of discrimination asserted by Charging Party Wendy Pincus and by the EEOC in this Lawsuit and deny that Defendants engaged in any wrongdoing or illegal activity and specifically dispute, among other things, that any Tutors are, or were, "employees" as the term "employee" is used in the ADEA and other federal and state anti-discrimination laws, instead of independent contractors, and therefore deny that the Tutor Applicants were subject to the ADEA and other similar federal and state anti-discrimination laws.

WHEREAS, the EEOC and Defendants have engaged in extensive settlement negotiations and have agreed that the Lawsuit should be resolved by entry of this Decree.

NOW, THEREFORE, in consideration of the mutual promises of each party to this Consent Decree (the "Decree"), the sufficiency of which is hereby acknowledged, it is agreed and **IT IS ORDERED, ADJUDGED, AND DECREED AS FOLLOWS**:

PART I GENERAL PROVISIONS

Section 101 Purpose of this Decree

A. The EEOC and Defendants desire to settle the Lawsuit, and therefore do hereby stipulate and consent to entry of this Decree as final and binding between the parties.

B. The Decree resolves all issues that were raised in the EEOC's Complaint (ECF No. 1), Amended Complaint (ECF NO. 8), and EEOC Charge of Discrimination number 556-2020-00511C, which served as the basis for this case. This Decree in no way affects the EEOC's right to process any pending or future charges that may have been or will be filed against Defendants, and to commence civil actions on any such charges. It is understood and agreed that all claims alleged in the Complaint and the underlying EEOC Charge of Discrimination number 556-2020-00511C, including the claims asserted by the EEOC in seeking relief for the Charging Party and Claimants, are resolved by this Decree.

C. Defendants attest that they are not currently employing or using the services of any Tutor (as defined herein), are not receiving or soliciting applications from Tutor Applicants (as defined herein), and have no plans to do so.

D. The EEOC and Defendants agree that this Court has jurisdiction over the subject matter of this litigation and the parties, that venue is proper, and that all administrative prerequisites have been met. No party will contest the validity of this Decree or the jurisdiction of the federal district court to enforce this Decree and its terms.

E. This Decree does not constitute an admission that any Defendant violated any local, state, or federal ordinance, regulation, ruling, statute, rule of decision, or principle of common law, or that any Person engaged in any improper or unlawful conduct or wrongdoing. The Decree or the payment of any money or other consideration in accord with this Decree will not be deemed or considered to be an admission or indication that any Person engaged in any improper or unlawful conduct or wrongdoing.

F. The terms of this Decree represent the full and complete agreement of the parties. The parties agree that this Decree may be entered into without Findings of Fact and Conclusions of Law being made and entered by the Court.

Section 102 Definitions

A. In this Decree the following terms will have the meanings assigned to them below unless otherwise specified:

1. "Answer" will mean the Amended Answer and Affirmative Defenses of iTutorGroup, Inc., and Tutor Group Limited, and the Answer and Affirmative Defenses of Shanghai Ping'An Intelligent Educations Technology Co. Ltd. filed in this Lawsuit as ECF No.18 and modified by Joint Stipulation at ECF No. 19.

2. "Complaint" will mean the Amended Complaint filed in this Lawsuit at ECF No. 8.

3. "Days" will mean calendar days.

4. "Effective Date" will mean the date this Decree is docketed by the Clerk of the Court after the Decree has been approved and "So Ordered" by the Court.

5. "Person" will mean any individual, partnership, limited liability company, limited liability partnership, joint venture, or governmental agency or any agency or political subdivision thereof, firm, corporation, association, trust, unincorporated organization or other entity.

6. "Pleadings" will mean the Complaint and the Answer.

7. "Lawsuit" will mean the above-captioned matter, *EEOC v. iTutorGroup, Inc. et al.*, Civil Action No. 1:22-cv-2565-PKC-PK.

8. "Resumption Date" means the earliest date a Defendant resumes soliciting, receiving, or considering applications for Tutor Applicants or similar positions.

9. "Resuming Defendant" will mean any Defendant that resumes soliciting, receiving, or considering applications from Tutor Applicants.

10. "Tutor Applicant" will mean any Person that applies to one or more of the Defendants to be a Tutor. However, "Tutor Applicant" does not include any Person that: (1) applies from a physical location outside the United States or, to the extent that the IP address can

reasonably be identified by the Resuming Defendant, from an IP address that appears to be from a physical location outside the United States; and (2) gives any Resuming Defendant the reasonable expectation of an intention to provide tutoring services from a physical location outside the United States. Tutor Applicant also does not include any Person that does not apply to any of the Resuming Defendants.

11. "Tutor" will mean any Person performing tutoring or similar services primarily from a physical location in the United States for or on behalf of any Resuming Defendant, even if such Person is providing services to students physically located in China or other locations outside the United States.

12. "US Tutor Business" will mean the operation of an electronic, online, or cloud-based platform or business by any of the Defendants whereby Tutors are hired by the Defendants to provide tutoring services.

Section 103 Applicability of Decree to Successors and Assigns or Upon Purchase, Merger, or Consolidation

A. Prior to any sale or other transfer of any business or assets to any entity that has the right to operate the US Tutor Business or establish its own US Tutor Business, Defendants will provide written notice of the Lawsuit, the Pleadings, and the Decree to any potential purchaser or potential transferee, including any entity with which any Defendant may merge or consolidate. Defendants will provide written notice to the EEOC at least twenty-one (21) days before any transfer or sale of any business or assets covered by this paragraph.

Section 104 Amendments to and Waivers Concerning this Decree

A. This Decree may be amended in the interests of justice and fairness and to facilitate execution of this Decree's provisions. No waiver, modification, or amendment of any provision of this Decree will be effective unless made in writing, approved by all parties to this Decree, and approved or ordered by the Court.

Section 105 Severability

A. If one or more provisions of the Decree are rendered or determined to be unlawful or unenforceable as a result of a legislative act or a decision by a court of competent jurisdiction, the provisions of this Decree that are not rendered unlawful, unenforceable, or incapable of performance will remain in full force and effect and the parties' responsibilities will not abate as to any and all provisions that have not been rendered unlawful or unenforceable, except to the extent that the intent of this Decree would be undermined.

Section 106 Breach of Decree; Governing Law

A. A breach of any term of this Decree by any Defendant will be deemed a material and substantive breach of this Decree. Nothing in this Decree will be construed to preclude the EEOC from bringing proceedings to enforce this Decree if any Defendant fails to perform any of the terms contained herein. This Decree will be governed by applicable federal law, as applied by the Eastern District of New York.

Section 107 Notices

A. Except as otherwise provided for in this Decree, all notifications, reports, and communications to the parties required under this Decree will be made in writing and will be sufficient as emailed to the following Persons (or their designated successors):

For the EEOC:

Daniel Seltzer
Trial Attorney
Equal Employment Opportunity Commission
New York District Office
daniel.seltzer@eeoc.gov
and

decreemonitor.nydo@eeoc.gov

For Defendants:

Michael J Sheppeard
SCARINCI HOLLENBECK LLC
150 Clove Road
9th Floor
Little Falls, NJ 07424
Email: msheppeard@sh-law.com

B. Any party may change such addresses by written notice to the other parties setting forth a new address for this purpose.

PART II INJUNCTIVE RELIEF

Section 201

201.1 Injunctions

A. Defendants, their managers, officers, agents, and any other Person acting on behalf of any Defendant, are hereby enjoined from rejecting Tutor Applicants age 40 or over because of age.

B. Defendants, their managers, officers, agents, and any other Person acting on behalf of any Defendant, are hereby enjoined from: (i) screening Tutor Applicants based on age; and (ii) requesting dates of birth for Tutor Applicants before a job offer is made. Notwithstanding anything herein to the contrary, the Defendants will be permitted to ask if the Tutor Applicant is over the age of eighteen (18) to determine compliance with any laws, regulations, or ordinances.

C. Defendants, their managers, officers, agents, affiliates, and any other Person acting on behalf of any Defendant, are hereby enjoined from rejecting Tutor Applicants because of sex or from screening applicants based on sex.

D. Defendants, their managers, officers, agents, affiliates, and any other acting on behalf of any Defendant, are hereby enjoined from retaliating against any employee, including but not limited to an employee who complains of discrimination, who opposes practices he or she considers to be unlawfully discriminatory with respect to Tutors or Tutor Applicants, and/or who participate in protected activity or who provide information related to complaints of discrimination regarding Tutors or Tutor Applicants.

E. At least seventy (70) days before the Resumption Date, a Defendant will provide notice to the EEOC that such Defendant intends to become a Resuming Defendant.

201.2 Posting and Distribution of Notices Concerning Lawsuit

A. Within fourteen (14) days of the Effective Date, Defendants will provide the "Notice of Lawsuit and Resolution" (attached as Exhibit A) to all individuals holding a c-level position with the Defendants, the members of the Board of Directors, and the head of human resources for each Defendant. Defendants will provide written notice to the EEOC within fourteen (14) days of the providing the Notice of Resolution pursuant to this provision.

B. Provision of Notice and Memo to Employees

1. No later than fifty-six (56) days before the Resumption Date, a Resuming Defendant will provide to the EEOC for the EEOC's approval a proposed a memo identifying the requirements of federal anti-discrimination laws, including prohibitions on age and sex discrimination in hiring (the "Resumption Memo").

2. No later than twenty-one (21) days before the Resumption Date, a Resuming Defendant will provide a copy of the Resumption Memo to all employees or independent contractors that may be involved in screening, hiring, or supervising Tutor Applicants or Tutors. Thereafter, the Resuming Defendant will provide the Resumption Memo to all future employees or independent contractors who may be involved in

screening, hiring, or supervising Tutor Applicants or Tutors within ten (10) days of the start of their employment or provision of services.

3. No later than ten (10) days after the first distribution required by the immediately preceding paragraph, a Resuming Defendant will provide written notice to the EEOC that it has directly distributed the Resumption Memo or caused to have the Resumption Memo distributed pursuant to Section 201.2.B.2.

4. On the Resumption Date and thereafter, a Resuming Defendant will either: (i) post the Resumption Memo or provide a link thereto on the website where Tutor Applicants apply; or (ii) upon submission of a completed application by a Tutor Applicant, provide each Tutor Applicant a copy of the Resumption Memo by email.

5. On the date that is six months after the Resumption Date and every six months thereafter, a Resuming Defendant will provide written notice to the EEOC confirming that it has distributed the Resumption Memo in accordance with Sections 201.2.B.2-B.4. The Resuming Defendant will also identify all employees or independent contractors that may be involved in screening, hiring, or supervising Tutor Applicants or Tutors to whom the Resumption Memo was distributed.

Section 202 Non-Discrimination Policy and Complaint Procedures

A. Content of Non-Discrimination Policies and Procedures

1. No later than fifty-six (56) days prior to the Resumption Date, a Resuming Defendant will provide the EEOC with proposed anti-discrimination policies and complaint procedures applicable to the screening, hiring, and supervision of Tutors and Tutor Applicants and setting forth the Resuming Defendant’s commitment to equal opportunity in all aspects of employment. The proposed policies and procedures will, at a minimum, substantively address the

following topics: (i) a detailed explanation of the prohibition against age and sex discrimination, including in hiring; (ii) the assurance that the Resuming Defendant will not retaliate against employees or applicants who complain of discrimination, who oppose practices they consider to be unlawfully discriminatory, and/or who participate in protected activity or who provide information related to complaints of discrimination; (iii) a clearly described complaint process that provides accessible avenues of complaint with a number of choices of individuals to whom complaints can be made, including individuals outside the employee's chain of command and individuals to whom Tutor Applicants or Tutors may complain, including by email; (iv) the designation of a senior manager or executive responsible for the Resuming Defendant's compliance with all EEO laws with respect to the screening and hiring of Tutor Applicants or Tutors; (v) the assurance that the Resuming Defendant will accept any and all complaints from employees or applicants who wish to file complaints; (vi) the assurance that the filing of anonymous complaints is permitted and include safeguards to preserve the anonymity when requested by a complainant; (vii) the assurance that the Resuming Defendant will keep confidential to the extent possible and not publicize unnecessarily the subject matter of the complaints or the identity of the complainants; (viii) a process that provides a prompt, thorough, and effective investigation, including interviewing the complainant and all witnesses and obtaining and reviewing all material documents identified by the complainant or respondent to the extent necessary to reach a reasonable conclusion concerning the allegations; (ix) a requirement that all aspects of an investigation be thoroughly documented in written form; (x) assurance that upon completion of an investigation into a discrimination complaint, the complainant and the respondent will promptly receive a summary of the conclusions reached as a result of the investigation; and

(xi) the assurance that the Resuming Defendant will take prompt and appropriate corrective action when it determines that discrimination has occurred ("Policies and Procedures").

B. Adoption and Issuance of Policies and Procedures

1. No later than twenty-one (21) days before the Resumption Date, a Resuming Defendant will: (i) formally adopt the Policies and Procedures; (ii) substantively incorporate the Policies and Procedures in its Employee Handbook; (iii) make the Policies and Procedures available on any company website that makes other human resources information or policies available to employees; and (iv) distribute to each employee a copy of the Policies and Procedures. Thereafter, each employee will be provided with the Policies and Procedures within ten (10) days of the commencement of such employee's employment.

2. No later than ten (10) days after the adoption and first distribution required by the immediately preceding paragraph, a Resuming Defendant will provide written notice to the EEOC that it has adopted and directly distributed the Policies and Procedures or caused to have the Policies and Procedures distributed pursuant to Section 202.B.1.

3. On the Resumption Date and thereafter, a Resuming Defendant will either: (i) post the Policies and Procedures or provide a link thereto on the website where Tutor Applicants apply; or (ii) upon submission of a completed application by a Tutor Applicant, provide each Tutor Applicant a copy of the Policies and Procedures by email.

4. On the date that is six months after the Resumption Date and every six months thereafter, a Resuming Defendant will provide written notice to the EEOC that it has distributed the Policies and Procedures in accordance with Section 202.B.1-3. The Resuming Defendant will also identify all employees or independent contractors that may be involved in

screening, hiring, or supervising Tutor Applicants or Tutors to whom the Policies and Procedures were distributed.

Section 203 Training

A. Initial Training

1. Timing and Requirements of Training

(i) A Resuming Defendant will be required to provide four-hour training programs conducted by third parties, both of which must be approved by the EEOC, for all supervisory and management employees, as well as any employees or independent contractors who may be involved in screening, hiring, or supervising Tutor Applicants and Tutors. The training programs will include: (a) a review of the obligations of Defendants under federal anti-discrimination laws and how such laws define unlawful discrimination with a focus on hiring and age- and sex-based discrimination; (b) instruction on the requirements of all Federal applicable equal opportunity laws including, but not limited to, Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Americans with Disabilities Act, the Equal Pay Act, and the Genetic Information Nondiscrimination Act; (c) a review of Defendants' Policies and Procedures; (d) examples of unlawful conduct, including age-based screening and rejection of applicants; and (e) instruction concerning an employee's or applicant's right to file with the EEOC (the "Training Program").

(ii) No later than fifty-six (56) days prior to the Resumption Date, a Resuming Defendant will submit to the EEOC for its approval the identity of the third party conducting the Training Program and all materials to be used by such third party for the Training Program. Such submission will contain: (a) a detailed agenda with all training materials; (b) curriculum vitae for the individual(s) who will conduct the training; and (c) a plan to ensure that all necessary Persons receive the required training.

(iii) No later than twenty-one (21) days before the Resumption Date, a Resuming Defendant will provide the Training Program to all supervisory and management employees, as well as any employees or independent contractors who may be involved in screening, hiring, or supervising Tutor Applicants or Tutors.

B. Continued Training and Training for New Employees

1. On the Resumption Date and thereafter, a Resuming Defendant will provide the Training Program to: (a) new supervisory and management employees, as well as any employees or independent contractors, who may be involved in screening, hiring, or supervising Tutor Applicants or Tutors, within thirty (30) days of the commencement of their employment or provision of services; and (b) on an annual basis no later than the anniversary of the Resumption Date, to all supervisory and management employees, as well as any employees or independent contractors who may be involved in screening, hiring, or supervising Tutor Applicants or Tutors.

C. Reporting Requirements for Training

1. All persons attending any training session described in the above paragraphs will print and sign their full names on an attendance sheet. Within ten (10) days of the completion of any Training Program described in Section 203.A.1.iii, a Resuming Defendant will provide the EEOC with copies of all attendance sheets and a then-current employee list.

2. On the date that is six months after the Resumption Date and every six months thereafter, a Resuming Defendant will provide the EEOC with attendance sheets for any Training Program described in Section 203.B.1 and a list of the employees, if any, who have not met their initial or annual requirements.

D. Pre-Training Notification Requirement

1. At least fourteen (14) days prior any Training Program that is required under this Section and is conducted live, a Resuming Defendant will provide the EEOC with written notice of the date, time, and location of the training. The EEOC, at its discretion and expense, may attend and observe such training.

Section 204 Monitoring and Reporting

A. Monitoring by the EEOC

1. The EEOC may monitor the compliance of any Resuming Defendant with this Decree through the inspection of the premises and records of the Defendant, and interviews with the Defendant's officers, agents, employees, and independent contractors at reasonable times. The Defendant will make available for inspection and copying any records related to this Decree upon request by the EEOC. Any activities undertaken by the EEOC pursuant to Section 204.A.1 will be at the EEOC's expense.

B. Reporting Requirements for Discrimination Complaints

1. On the date that is the Resumption Date and every six months thereafter, a Resuming Defendant will provide written notice to the EEOC concerning any verbal or written complaints of discrimination from employees or applicants that were received, pending, or closed during the preceding six months. Such written notice will include the name of the complainant; a list of each step taken by the Resuming Defendant during the investigation; a summary of the complaint, the location; the results of any investigation of the complaint; and any remedial action taken by the Resuming Defendant.

C. Delay in Approvals by the EEOC

1. To the extent any document or performance of an action must be approved by the EEOC, the EEOC will provide a written response no later than ten (10) days from the request for approval. That response may be an approval, a denial of approval, or a request that Defendant modify the document or action. For every day beyond ten (10) days that the EEOC delays a response, the immediately subsequent deadline that is dependent on the approval of the EEOC will be extended by an additional day.

Section 205 Compliance with Record-keeping Requirements

A. Defendants agree to maintain such records required by 29 C.F.R. §1602 et seq. (to the extent that such is applicable) and such records as are reasonable and necessary to demonstrate their compliance with this Decree and to verify that written notices submitted pursuant to this Decree are accurate.

PART III MONETARY RELIEF

Section 301 Monetary Payment to Claimants and Hiring Preference

A. Within twenty-one (21) days of the Effective Date, Defendants will pay or cause to be paid the total gross sum of $365,000 (the "Settlement Amount") to American Legal Claim Services, LLC ("Claims Administrator") to be placed in a segregated, interest-bearing Qualified Settlement Fund ("Claims Fund") under Section 468(b) of the Internal Revenue Code.

B. The Settlement Amount will be distributed among certain Tutor Applicants who: (1) were allegedly rejected by Defendants because of age in March and April 2020; and (2) provide the EEOC with the necessary information needed for the EEOC to determine their eligibility and facilitate payment ("Claimants"). The distribution of the Settlement Amount to the Claimants will be at the EEOC's sole discretion; Defendants may not challenge the distribution to the Claimants in any way.

C. Defendants will provide the EEOC with any reasonably necessary information requested that is in the possession, custody, or control of the Defendants, including all contact information any of the Defendants may have for Claimants and other persons that are reasonably believed to be potential Claimants.

D. For each gross payment received by a Claimant, half of such payment will be treated as compensatory damages and half will be treated as backpay.

E. In order to receive payment, Claimants will sign a release in the form attached hereto as Exhibit B and provide the signed release to the Claims Administrator. A copy of all signed releases will be provided to Defendants.

F. At a time or times of the EEOC's choosing, the EEOC will cause the Claims Administrator to send checks for compensatory damages and IRS form 1099 via certified or other trackable mail to the Claimants identified by EEOC.

G. At a time or times of the EEOC's choosing, the EEOC will cause Claims Administrator to send checks for backpay (the "Backpay Payment") and IRS form W-2 via certified or other trackable mail to the Claimants identified by the EEOC. The Claims Administrator will make all required withholdings for applicable federal, state, and local income taxes and the Claimant's share of federal payroll taxes from the Backpay Payment. Defendants will be responsible for any tax obligation Defendants incur from of these payments, including the employer's share of federal payroll taxes, with such amounts being in addition to Defendants' payment in Paragraph 301.A, above.

H. Defendants will be solely liable for the Claims Administrator's expenses. This liability is in addition to the payment described in Paragraph 301.A, above.

I. No later than twenty-one (21) days before the Resumption Date, a Resuming Defendant will contact by email all applicants who were purportedly rejected by Defendants because of age in March and April 2020, provide the Notice of Lawsuit and Resolution, and invite them to reapply. The text of the email must be provided to the EEOC for its approval no later than fifty-six (56) days before the Resumption Date. The EEOC may supply additional email addresses for such applicants.

J. A Resuming Defendant will interview any applicants notified in Paragraph 301.I who reapply.

K. Within two months of the Resumption Date, a Resuming Defendant will provide a report to the EEOC that includes the following information: (1) the names and contact information of all applicants who were rejected by Defendants because of age in March and April 2020 and who reapplied; (2) the outcome of each applicant's application and interview; and (3) to the extent any applicant who reapplied was not offered a tutoring position, a detailed explanation as to why an offer was not made.

Section 302: The EEOC's Reporting Requirements under IRC Sections 162(f) and 6050X

A. The EEOC may be required to report the fact of this settlement to the Internal Revenue Service ("IRS") under Section 162(f) and 6050X of the Internal Revenue Code, which allow for certain payments by employers to be deducted from the employer's taxes. If the EEOC is required to do so, the EEOC will provide Defendants with a copy of the 1098-F form that it will provide to the IRS.

B. Defendant iTutorGroup, Inc.'s EIN is 46-5430481. Defendants Shanghai Ping and

Tutor Group Limited do not have EINs.

C. If the EEOC is required to issue form 1098-F to any of the Defendants, the EEOC will send a copy, by regular mail and email, to:

Michael J Sheppeard
SCARINCI HOLLENBECK LLC
150 Clove Road
9th Floor
Little Falls, NJ 07424
Email: msheppeard@sh-law.com

D. The EEOC has made no representations regarding whether the amount paid pursuant to this settlement qualifies for the deduction under the Internal Revenue Code. The provision of the Form 1098-F by the EEOC does not mean that the requirements to claim a deduction under the Internal Revenue Code have been met. Any decision about a deduction pursuant to the Internal Revenue Code will be made solely by the IRS with no input from the EEOC. The parties are not acting in reliance on any representations made by the EEOC regarding whether the amounts paid pursuant to this Decree qualify for a deduction under the Internal Revenue Code.

PART IV SIGNATURES

A. Each signatory to this Decree represents that (s)he is fully authorized to execute this Decree and to bind the parties on whose behalf (s)he signs.

PART V DURATION OF DECREE

A. This Decree will remain in effect for five (5) years from the Effective Date of this Decree or three (3) years from the Resumption Date, whichever is later; provided, however, that in the event that: (1) the EEOC has notified Defendants in writing not less than twenty-one (21) days in advance of the expiration of this Decree that any Defendant is not in compliance with any section of this Decree and providing reasonable detail of such non-compliance; or (2) there is an enforcement action pending concerning this Decree by the EEOC against any Defendant, this Decree will remain in effect against Defendants until the EEOC determines that Defendants are in compliance or such enforcement action is resolved.

B. The Court will retain jurisdiction over this lawsuit for all purposes including, but not limited to, the entering of all orders, judgments, and decrees as necessary to implement the relief provided herein. Upon the Effective Date, the matter may be administratively closed but will not be dismissed.

C. In the event that any party to this Decree believes that any other party has failed to comply with any provision(s) of the Decree, the complaining party will notify the allegedly non-complying party in writing of the alleged non-compliance within fourteen (14) days of learning of the alleged non-compliance and will afford the alleged non-complying party fourteen (14) days to remedy the non-compliance or otherwise demonstrate compliance. If the alleged non-complying party has not remedied the alleged non-compliance within fourteen (14) days, the complaining party may apply to the Court for appropriate relief. This paragraph will not apply to the EEOC in the event that it determines that providing such notice concerning the alleged non-compliance will negatively affect the public interest.

D. Solicitations by third parties will not be subject to this Consent Decree if no Defendant has control or involvement in the solicitations. Solicitations by a Defendant or by third parties where a Defendant has control or involvement in the solicitations will not be subject to this Consent Decree if: (1) Defendants exercise reasonable means to ensure that such solicitations are not accessible to individuals in the United States; or (2) where such reasonable means are not available or may be ineffective, Defendants ensure that highly visible disclaimers are posted on the solicitations making it clear that they are not intended for applicants from the United States.

E. Once the Consent Decree is no longer in effect, Defendants may request that the EEOC execute a stipulation of discontinuance with prejudice and the EEOC will provide such within ten (10) days of such request.

APPROVED IN FORM AND CONTENT:

For Plaintiff EEOC:

Jeffrey Burstein

JEFFREY BURSTEIN
Regional Attorney
U.S. EQUAL EMPLOYMENT
OPPORTUNITY COMMISSION
New York District Office
33 Whitehall Street, 5th Floor
New York, NY 10004-2112
(212) 336-3770
jeffrey.burstein@eeoc.gov

For Defendants:

SCARINCI HOLLENBECK LLC
Michael J Sheppeard

589 8th Avenue, 16th Floor
New York, NY 10018
Ph.: (212) 286-0747
msheppeard@sh-law.com

SO ORDERED this _____ day of August, 2023.

____
Hon. Pamela K. Chen
United States District Judge

EXHIBIT A: Notice

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
New York District Office

33 Whitehall Street, 5th Floor
New York, NY 10004-2112
(212) 336-3620
TTY (212) 336-3622
General FAX (212) 336-3625

NOTICE TO ALL EMPLOYEES OF LAWSUIT & SETTLEMENT

This Notice is being posted pursuant to a Consent Decree entered in resolution of a lawsuit brought by the U.S. Equal Employment Opportunity Commission (the "EEOC") in federal court in the Eastern District of New York. In its lawsuit, the EEOC alleged that Defendants iTutorGroup, Inc.; Shanghai Ping'An Intelligent Education Technology Co., Ltd.; and Tutor Group Limited—providers of English-language tutoring services to students in China under the "iTutorGroup" brand name—programmed their application software to automatically reject female applicants over the age of 55 and male applicants over the age of 60 and that in early 2020, Defendants failed to hire more than 200 qualified tutor applicants age 55 and older from the United States because of their age.

Defendants iTutorGroup, Inc.; Shanghai Ping'An Intelligent Education Technology Co., Ltd.; and Tutor Group Limited denied the EEOC's allegations in their entirety, denied that any of the Defendants were engaged in any wrongdoing or illegal activity, and asserted numerous affirmative defenses.

The EEOC and Defendants have engaged in extensive settlement negotiations and have agreed that the Lawsuit should be resolved by entry of the Consent Decree.

Federal law prohibits employers from discriminating against applicants and employees based on age, national origin, religion, race, color, sex, disability, or genetic information. Defendants, and their managers, officers, and agents, will support and comply with Federal law prohibiting discrimination against any employee or applicant for employment because of an individual's age.

Pursuant to the Consent Decree, Defendants paid money damages to the claimants who were allegedly subject to discrimination, provided this notice to certain executives and human resources employees, and upon the resumption of United States-based tutoring:

1. Are enjoined from engaging in age- or sex-based discrimination against United States-based tutoring applicants or retaliation against any person

who exercises his or her rights under United States Federal anti-discrimination laws;

2. Will maintain and distribute written policies and procedures prohibiting discrimination and enabling United States-based tutoring applicants and United States-based tutors to file discrimination complaints;

3. Must provide training on United States Federal laws prohibiting employment age- and sex-based discrimination in hiring to all managers and employees involved in hiring United States-based tutoring applicants and United States-based tutors;

4. Must permit the EEOC to monitor compliance with the Consent Decree; and

5. Will provide the EEOC with periodic reports on complaints of discrimination concerning United States-based tutoring applicants and United States-based tutors.

Should you have any complaints or questions regarding employment discrimination, contact the EEOC at:

Equal Employment Opportunity Commission
(800) 669-4000
Website: www.eeoc.gov

Dated:________________

THIS IS AN OFFICIAL NOTICE AND MUST NOT BE ALTERED OR DEFACED BY ANYONE OR COVERED BY ANY OTHER MATERIAL

The Consent Decree remains in effect for five (5) years from its effective date or three (3) years from the date that any Defendant resumes United States-based tutoring. Any questions concerning this Notice or compliance with its provisions may be directed to the U.S. Equal Employment Opportunity Commission at the number listed above.

Exhibit B: Release Language

In consideration for money paid to me by Defendants iTutorGroup, Inc.; Shanghai Ping'An Intelligent Education Technology Co., Ltd.; and Tutor Group Limited (collectively, "Defendants") in connection with the resolution of *EEOC v. iTutorGroup, Inc. et al.*, Civil Action No. 1:22-cv-2565-PKC-PK, I remise, release, waive, and forever discharge my right to recover for any claims of age-based discriminatory hiring that I had prior to the date of this release that (i) arose under the Age Discrimination in Employment Act against Defendants iTutorGroup, Inc., Shanghai Ping'An Intelligent Education Technology Co., Ltd., and Tutor Group Limited, whether jointly and/or severally, and (ii) were included in the claims alleged in the EEOC's complaint, as the same may have been amended, *in EEOC v. iTutorGroup, Inc. et al.*, Civil Action No. 1:22-cv-2565-PKC-PK

Date: ______________________________ Printed Name:______________________________

Signature:______________________________

AB-331 Automated decision tools. (2023-2024)

As Amends the Law Today

SECTION 1. *Chapter 25 (commencing with Section 22756) is added to Division 8 of the Business and Professions Code, to read:*

CHAPTER 25. Automated Decision Tools

22756. *As used in this chapter:*

(a) "Algorithmic discrimination" means the condition in which an automated decision tool contributes to unjustified differential treatment or impacts disfavoring people based on their actual or perceived race, color, ethnicity, sex, religion, age, national origin, limited English proficiency, disability, veteran status, genetic information, reproductive health, or any other classification protected by state law.

(b) "Artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing a real or virtual environment.

(c) "Automated decision tool" means a system or service that uses artificial intelligence and has been specifically developed and marketed to, or specifically modified to, make, or be a controlling factor in making, consequential decisions.

(d) "Consequential decision" means a decision or judgment that has a legal, material, or similarly significant effect on an individual's life relating to the impact of, access to, or the cost, terms, or availability of, any of the following:

(1) Employment, workers management, or self-employment, including, but not limited to, all of the following:

(A) Pay or promotion.

(B) Hiring or termination.

(C) Automated task allocation.

(2) Education and vocational training, including, but not limited to, all of the following:

(A) Assessment, including, but not limited to, detecting student cheating or plagiarism.

(B) Accreditation.

(C) Certification.

(D) Admissions.

(E) Financial aid or scholarships.

(3) Housing or lodging, including rental or short-term housing or lodging.

(4) Essential utilities, including electricity, heat, water, internet or telecommunications access, or transportation.

(5) Family planning, including adoption services or reproductive services, as well as assessments related to child protective services.

(6) Health care or health insurance, including mental health care, dental, or vision.

(7) Financial services, including a financial service provided by a mortgage company, mortgage broker, or creditor.

(8) The criminal justice system, including, but not limited to, all of the following:

(A) Risk assessments for pretrial hearings.

(B) Sentencing.

(C) Parole.

(9) Legal services, including private arbitration or mediation.

(10) Voting.

(11) Access to benefits or services or assignment of penalties.

(e) "Deployer" means a person, partnership, state or local government agency, or corporation that uses an automated decision tool to make a consequential decision.

(f) "Developer" means a person, partnership, state or local government agency, or corporation that designs, codes, or produces an automated decision tool, or substantially modifies an artificial intelligence system or service for the intended purpose of making, or being a controlling factor in making, consequential decisions, whether for its own use or for use by a third party.

(g) "Impact assessment" means a documented risk-based evaluation of an automated decision tool that meets the criteria of Section 22756.1.

(h) "Sex" includes pregnancy, childbirth, and related conditions, gender identity, intersex status, and sexual orientation.

(i) "Significant update" means a new version, new release, or other update to an automated decision tool that includes changes to its use case, key functionality, or expected outcomes.
22756.1. *(a) On or before January 1, 2025, and annually thereafter, a deployer of an automated decision tool shall perform an impact assessment for any automated decision tool the deployer uses that includes all of the following:*

(1) A statement of the purpose of the automated decision tool and its intended benefits, uses, and deployment contexts.

(2) A description of the automated decision tool's outputs and how they are used to make, or be a controlling factor in making, a consequential decision.

(3) A summary of the type of data collected from natural persons and processed by the automated decision tool when it is used to make, or be a controlling factor in making, a consequential decision.

(4) A statement of the extent to which the deployer's use of the automated decision tool is consistent with or varies from the statement required of the developer by Section 22756.3.

(5) An analysis of potential adverse impacts on the basis of sex, race, color, ethnicity, religion, age, national origin, limited English proficiency, disability, veteran status, or genetic information from the deployer's use of the automated decision tool.

(6) A description of the safeguards implemented, or that will be implemented, by the deployer to address any reasonably foreseeable risks of algorithmic discrimination arising from the use of the automated decision tool known to the deployer at the time of the impact assessment.

(7) A description of how the automated decision tool will be used by a natural person, or monitored when it is used, to make, or be a controlling factor in making, a consequential decision.

(8) A description of how the automated decision tool has been or will be evaluated for validity or relevance.

(b) On or before January 1, 2025, and annually thereafter, a developer of an automated decision tool shall complete and document an assessment of any automated decision tool that it designs, codes, or produces that includes all of the following:

(1) A statement of the purpose of the automated decision tool and its intended benefits, uses, and deployment contexts.

(2) A description of the automated decision tool's outputs and how they are used to make, or be a controlling factor in making, a consequential decision.

(3) A summary of the type of data collected from natural persons and processed by the automated decision tool when it is used to make, or be a controlling factor in making, a consequential decision.

(4) An analysis of a potential adverse impact on the basis of sex, race, color, ethnicity, religion, age, national origin, limited English proficiency, disability, veteran status, or genetic information from the deployer's use of the automated decision tool.

(5) A description of the measures taken by the developer to mitigate the risk known to the developer of algorithmic discrimination arising from the use of the automated decision tool.

(6) A description of how the automated decision tool can be used by a natural person, or monitored when it is used, to make, or be a controlling factor in making, a consequential decision.

(c) A deployer or developer shall, in addition to the impact assessment required by subdivisions (a) and (b), perform, as soon as feasible, an impact assessment with respect to any significant update.

(d) This section does not apply to a deployer with fewer than 25 employees unless, as of the end of the prior calendar year, the deployer deployed an automated decision tool that impacted more than 999 people per year.

22756.2. *(a) (1) A deployer shall, at or before the time an automated decision tool is used to make a consequential decision, notify any natural person that is the subject of the consequential decision that an automated decision tool is being used to make, or be a controlling factor in making, the consequential decision.*

(2) A deployer shall provide to a natural person notified pursuant to this subdivision all of the following:

(A) A statement of the purpose of the automated decision tool.

(B) Contact information for the deployer.

(C) A plain language description of the automated decision tool that includes a description of any human components and how any automated component is used to inform a consequential decision.

(b) (1) If a consequential decision is made solely based on the output of an automated decision tool, a deployer shall, if technically feasible, accommodate a natural person's request to not be subject to the automated decision tool and to be subject to an alternative selection process or accommodation.

(2) After a request pursuant to paragraph (1), a deployer may reasonably request, collect, and process information from a natural person for the purposes of identifying the person and the associated consequential decision. If the person does not provide that information, the deployer shall not be obligated to provide an alternative selection process or accommodation.

22756.3. *(a) A developer shall provide a deployer with a statement regarding the intended uses of the automated decision tool and documentation regarding all of the following:*

(1) The known limitations of the automated decision tool, including any reasonably foreseeable risks of algorithmic discrimination arising from its intended use.

(2) A description of the type of data used to program or train the automated decision tool.

(3) A description of how the automated decision tool was evaluated for validity and explainability before sale or licensing.

(b) This section does not require the disclosure of trade secrets, as defined in Section 3426.1 of the Civil Code.

22756.4. *(a) (1) A deployer or developer shall establish, document, implement, and maintain a governance program that contains reasonable administrative and technical safeguards to map, measure, manage, and govern the reasonably foreseeable risks of algorithmic discrimination associated with the use or intended use of an automated decision tool.*

(2) The safeguards required by this subdivision shall be appropriate to all of the following:

(A) The use or intended use of the automated decision tool.

(B) The deployer’s or developer’s role as a deployer or developer.

(C) The size, complexity, and resources of the deployer or developer.

(D) The nature, context, and scope of the activities of the deployer or developer in connection with the automated decision tool.

(E) The technical feasibility and cost of available tools, assessments, and other means used by a deployer or developer to map, measure, manage, and govern the risks associated with an automated decision tool.

(b) The governance program required by this section shall be designed to do all of the following:

(1) (A) Designate at least one employee to be responsible for overseeing and maintaining the governance program and compliance with this chapter.

(B) (i) An employee designated pursuant to this paragraph shall have the authority to assert to the employee’s employer a good faith belief that the design, production, or use of an automated decision tool fails to comply with the requirements of this chapter.

(ii) An employer of an employee designated pursuant to this paragraph shall conduct a prompt and complete assessment of any compliance issue raised by that employee.

(2) Identify and implement safeguards to address reasonably foreseeable risks of algorithmic discrimination resulting from the use or intended use of an automated decision tool.

(3) If established by a deployer, provide for the performance of impact assessments as required by Section 22756.1.

(4) If established by a developer, provide for compliance with Sections 22756.2 and 22756.3.

(5) Conduct an annual and comprehensive review of policies, practices, and procedures to ensure compliance with this chapter.

(6) Maintain for two years after completion the results of an impact assessment.

(7) Evaluate and make reasonable adjustments to administrative and technical safeguards in light of material changes in technology, the risks associated with the automated decision tool, the state of technical standards, and changes in business arrangements or operations of the deployer or developer.

(c) This section does not apply to a deployer with fewer than 25 employees unless, as of the end of the prior calendar year, the deployer deployed an automated decision tool that impacted more than 999 people per year.

22756.5. *A deployer or developer shall make publicly available, in a readily accessible manner, a clear policy that provides a summary of both of the following:*

(a) The types of automated decision tools currently in use or made available to others by the deployer or developer.

(b) How the deployer or developer manages the reasonably foreseeable risks of algorithmic discrimination that may arise from the use of the automated decision tools it currently uses or makes available to others.

22756.6. *(a) A deployer shall not use an automated decision tool that results in algorithmic discrimination.*

(b) (1) On and after January 1, 2026, a person may bring a civil action against a deployer for violation of this section.

(2) In an action brought pursuant to paragraph (1), the plaintiff shall have the burden of proof to demonstrate that the deployer’s use of the automated decision tool resulted in algorithmic discrimination that caused actual harm to the person bringing the civil action.

(c) In addition to any other remedy at law, a deployer that violates this section shall be liable to a prevailing plaintiff for any of the following:

(1) Compensatory damages.

(2) Declaratory relief.

(3) Reasonable attorney's fees and costs.

22756.7. *(a) Within 60 days of completing an impact assessment required by this chapter, a deployer or a developer shall provide the impact assessment to the Civil Rights Department.*

(b) (1) A deployer or developer who violates this section shall be liable for an administrative fine of not more than ten thousand dollars ($10,000) per violation in an administrative enforcement action brought by the Civil Rights Department.

(2) Each day on which an automated decision tool is used for which an impact assessment has not been submitted pursuant to this section shall give rise to a distinct violation of this section.

(c) The Civil Rights Department may share impact assessments with other state entities as appropriate.

22756.8. *(a) (1) Any of the following public attorneys may bring a civil action against a deployer or developer for a violation of this chapter:*

(A) The Attorney General in the name of the people of the State of California.

(B) A district attorney, county counsel, or city attorney for the jurisdiction in which the violation occurred.

(C) A city prosecutor in any city having a full-time city prosecutor, with the consent of the district attorney.

(2) A court may award in an action brought pursuant to this subdivision all of the following:

(A) Injunctive relief.

(B) Declaratory relief.

(C) Reasonable attorney's fees and litigation costs.

(b) (1) A public attorney, before commencing an action pursuant to this section for injunctive relief, shall provide 45 days' written notice to a deployer or developer of the alleged violations of this chapter.

(2) (A) The developer or deployer may cure, within 45 days of receiving the written notice described in paragraph (1), the noticed violation and provide the person who gave the notice an express written statement, made under penalty of perjury, that the violation has been cured and that no further violations shall occur.

(B) If the developer or deployer cures the noticed violation and provides the express written statement pursuant to subparagraph (A), a claim for injunctive relief shall not be maintained for the noticed violation.

SEC. 2. *No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution for certain costs that may be incurred by a local agency or school district because, in that regard, this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.*

However, if the Commission on State Mandates determines that this act contains other costs mandated by the state, reimbursement to local agencies and school districts for those costs shall be made pursuant to Part 7 (commencing with Section 17500) of Division 4 of Title 2 of the Government Code.

OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.

My Administration places the highest urgency on governing the development and use of AI safely and responsibly, and is therefore advancing a coordinated, Federal Government-wide approach to doing so. The rapid speed at which AI capabilities are advancing compels the United States to lead in this moment for the sake of our security, economy, and society.

In the end, AI reflects the principles of the people who build it, the people who use it, and the data upon which it is built. I firmly believe that the power of our ideals; the foundations of our society; and the creativity, diversity, and decency of our people are the reasons that America thrived in past eras of rapid change. They are the reasons we will succeed again in this moment. We are more than capable of harnessing AI for justice, security, and opportunity for all.

Sec. 2. Policy and Principles. It is the policy of my Administration to advance and govern the development and use of AI in accordance with eight guiding principles and priorities. When undertaking the actions set forth in this order, executive departments and agencies (agencies) shall, as appropriate and consistent with applicable law, adhere to these principles, while, as feasible, taking into account the views of other agencies, industry, members of academia, civil society, labor unions, international allies and partners, and other relevant organizations:

(a) Artificial Intelligence must be safe and secure. Meeting this goal requires robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use. It also requires addressing AI systems' most pressing security risks — including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers — while navigating AI's opacity and complexity. Testing and evaluations, including post-deployment performance monitoring, will help ensure that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed and operated in a secure manner, and are compliant with applicable Federal laws and policies. Finally, my Administration will help develop effective labeling and content provenance mechanisms, so that Americans are able to determine when content is generated using AI and when it is not. These actions will provide a vital foundation for an approach that addresses AI's risks without unduly reducing its benefits.

(b) Promoting responsible innovation, competition, and collaboration will allow the United States to lead in AI and unlock the technology's potential to solve some of society's most difficult challenges. This effort requires investments in AI-related education, training, development, research, and capacity, while simultaneously tackling novel intellectual property (IP) questions and other problems to protect inventors and creators. Across the Federal Government, my Administration will support programs to provide Americans the skills they need for the age of AI and attract the world's AI talent to our shores — not just to study, but to stay — so that the companies and technologies of the future are made in America. The Federal Government will promote a fair, open, and competitive ecosystem and marketplace for AI and related technologies so that small developers and entrepreneurs can continue to drive innovation. Doing so requires stopping unlawful collusion and addressing risks from dominant firms' use of key assets such as semiconductors, computing power, cloud storage, and data to disadvantage competitors, and it requires supporting a marketplace that harnesses the benefits of AI to provide new opportunities for small businesses, workers, and entrepreneurs.

(c) The responsible development and use of AI require a commitment to supporting American workers. As AI creates new jobs and industries, all workers need a seat at the table, including through collective bargaining, to ensure that they benefit from these opportunities. My Administration will seek to adapt job training and education to support a diverse workforce and help provide access to opportunities that AI creates. In the workplace itself, AI should not be deployed in ways that undermine rights, worsen job quality, encourage undue worker surveillance, lessen market competition, introduce new health and safety risks, or cause harmful labor-force disruptions. The critical next steps in AI development should be built on the views of workers, labor unions, educators, and employers to support responsible uses of AI that improve workers' lives, positively augment human work, and help all people safely enjoy the gains and opportunities from technological innovation.

(d) Artificial Intelligence policies must be consistent with my Administration's dedication to advancing equity and civil rights. My Administration cannot — and will not — tolerate the use of AI to disadvantage those who are already too often denied equal opportunity and justice. From hiring to housing to healthcare, we have seen what happens when AI use deepens discrimination and bias, rather than improving quality of life. Artificial Intelligence systems deployed irresponsibly have reproduced and intensified existing inequities, caused new types of harmful discrimination, and exacerbated online and physical harms. My Administration will build on the important steps that have already been taken — such as issuing the Blueprint for an AI Bill of Rights, the AI Risk Management Framework, and Executive Order 14091 of February 16, 2023 (Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government) — in seeking to ensure that AI complies with all Federal laws and to promote robust technical evaluations, careful oversight, engagement with affected communities, and rigorous regulation. It is necessary to hold those developing and deploying AI accountable to standards that protect against unlawful discrimination and abuse, including in the justice system and the Federal Government. Only then can Americans trust AI to advance civil rights, civil liberties, equity, and justice for all.

(e) The interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected. Use of new technologies, such as AI, does not excuse organizations from their legal obligations, and hard-won consumer protections are more important than ever in moments of technological change. The Federal Government will enforce existing consumer protection laws and principles and enact appropriate safeguards against fraud, unintended bias, discrimination, infringements on privacy, and other harms from AI. Such protections are especially important in critical fields like healthcare, financial services, education, housing, law, and transportation, where mistakes by or misuse of AI could harm patients, cost consumers or small businesses, or jeopardize safety or rights. At the same time, my Administration will promote responsible uses of AI that protect consumers, raise the quality of goods and services, lower their prices, or expand selection and availability.

(f) Americans' privacy and civil liberties must be protected as AI continues advancing. Artificial Intelligence is making it easier to extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires. Artificial Intelligence's capabilities in these areas can increase the risk that personal data could be exploited and exposed. To combat this risk, the Federal Government will ensure that the collection, use, and retention of data is lawful, is secure, and mitigates privacy and confidentiality risks. Agencies shall use available policy and technical tools, including privacy-enhancing technologies (PETs) where appropriate, to protect privacy and to combat the broader legal and societal risks — including the chilling of First Amendment rights — that result from the improper collection and use of people's data.

(g) It is important to manage the risks from the Federal Government's own use of AI and increase its internal capacity to regulate, govern, and support responsible use of AI to deliver better results for Americans. These efforts start with people, our Nation's greatest asset. My Administration will take steps to attract, retain, and develop public service-oriented AI professionals, including from underserved communities, across disciplines — including technology, policy, managerial, procurement, regulatory, ethical, governance, and legal fields — and ease AI professionals' path into the Federal Government to help harness and govern AI. The Federal Government will work to ensure that all members of its workforce receive adequate training to understand the benefits, risks, and limitations of AI for their job functions, and to modernize Federal Government information technology infrastructure, remove bureaucratic obstacles, and ensure that safe and rights-respecting AI is adopted, deployed, and used.

(h) The Federal Government should lead the way to global societal, economic, and technological progress, as the United States has in previous eras of disruptive innovation and change. This leadership is not measured solely by the technological advancements our country makes. Effective leadership also means pioneering those systems and safeguards needed to deploy technology responsibly — and building and promoting those safeguards with the rest of the world. My Administration will engage with international allies and partners in developing a framework to manage AI's risks, unlock AI's potential for good, and promote common approaches to shared challenges. The Federal Government will seek to promote responsible AI safety and security principles and actions with other nations, including our competitors, while leading key global conversations and collaborations to ensure that AI benefits the whole world, rather than exacerbating inequities, threatening human rights, and causing other harms.

Sec. 3. Definitions. For purposes of this order:

(a) The term "agency" means each agency described in 44 U.S.C. 3502(1), except for the independent regulatory agencies described in 44 U.S.C. 3502(5).

(b) The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

(c) The term “AI model” means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

(d) The term “AI red-teaming” means a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI. Artificial Intelligence red-teaming is most often performed by dedicated “red teams” that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.

(e) The term “AI system” means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

(f) The term “commercially available information” means any information or data about an individual or group of individuals, including an individual’s or group of individuals’ device or location, that is made available or obtainable and sold, leased, or licensed to the general public or to governmental or non-governmental entities.

(g) The term “crime forecasting” means the use of analytical techniques to attempt to predict future crimes or crime-related information. It can include machine-generated predictions that use algorithms to analyze large volumes of data, as well as other forecasts that are generated without machines and based on statistics, such as historical crime statistics.

(h) The term “critical and emerging technologies” means those technologies listed in the February 2022 Critical and Emerging Technologies List Update issued by the National Science and Technology Council (NSTC), as amended by subsequent updates to the list issued by the NSTC.

(i) The term “critical infrastructure” has the meaning set forth in section 1016(e) of the USA PATRIOT Act of 2001, 42 U.S.C. 5195c(e).

(j) The term “differential-privacy guarantee” means protections that allow information about a group to be shared while provably limiting the improper access, use, or disclosure of personal information about particular entities.

(k) The term “dual-use foundation model” means an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters, such as by:

(i) substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons;

(ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks; or

(iii) permitting the evasion of human control or oversight through means of deception or obfuscation.

Models meet this definition even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities.

(l) The term “Federal law enforcement agency” has the meaning set forth in section 21(a) of Executive Order 14074 of May 25, 2022 (Advancing Effective, Accountable Policing and Criminal Justice Practices To Enhance Public Trust and Public Safety).

(m) The term “floating-point operation” means any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base.

(n) The term “foreign person” has the meaning set forth in section 5(c) of Executive Order 13984 of January 19, 2021 (Taking Additional Steps To

Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities).

(o) The terms “foreign reseller” and “foreign reseller of United States Infrastructure as a Service Products” mean a foreign person who has established an Infrastructure as a Service Account to provide Infrastructure as a Service Products subsequently, in whole or in part, to a third party.

(p) The term “generative AI” means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

(q) The terms “Infrastructure as a Service Product,” “United States Infrastructure as a Service Product,” “United States Infrastructure as a Service Provider,” and “Infrastructure as a Service Account” each have the respective meanings given to those terms in section 5 of Executive Order 13984.

(r) The term “integer operation” means any mathematical operation or assignment involving only integers, or whole numbers expressed without a decimal point.

(s) The term “Intelligence Community” has the meaning given to that term in section 3.5(h) of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended.

(t) The term “machine learning” means a set of techniques that can be used to train AI algorithms to improve performance at a task based on data.

(u) The term “model weight” means a numerical parameter within an AI model that helps determine the model’s outputs in response to inputs.

(v) The term “national security system” has the meaning set forth in 44 U.S.C. 3552(b)(6).

(w) The term “omics” means biomolecules, including nucleic acids, proteins, and metabolites, that make up a cell or cellular system.

(x) The term “Open RAN” means the Open Radio Access Network approach to telecommunications-network standardization adopted by the O-RAN Alliance, Third Generation Partnership Project, or any similar set of published open standards for multi-vendor network equipment interoperability.

(y) The term “personally identifiable information” has the meaning set forth in Office of Management and Budget (OMB) Circular No. A-130.

(z) The term “privacy-enhancing technology” means any software or hardware solution, technical process, technique, or other technological means of mitigating privacy risks arising from data processing, including by enhancing predictability, manageability, disassociability, storage, security, and confidentiality. These technological means may include secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy, and synthetic-data-generation tools. This is also sometimes referred to as “privacy-preserving technology.”

(aa) The term “privacy impact assessment” has the meaning set forth in OMB Circular No. A-130.

(bb) The term “Sector Risk Management Agency” has the meaning set forth in 6 U.S.C. 650(23).

(cc) The term “self-healing network” means a telecommunications network that automatically diagnoses and addresses network issues to permit self-restoration.

(dd) The term “synthetic biology” means a field of science that involves redesigning organisms, or the biomolecules of organisms, at the genetic level to give them new characteristics. Synthetic nucleic acids are a type of biomolecule redesigned through synthetic-biology methods.

(ee) The term “synthetic content” means information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI.

(ff) The term “testbed” means a facility or mechanism equipped for conducting rigorous, transparent, and replicable testing of tools and technologies, including AI and PETs, to help evaluate the functionality, usability, and performance of those tools or technologies.

(gg) The term "watermarking" means the act of embedding information, which is typically difficult to remove, into outputs created by AI — including into outputs such as photos, videos, audio clips, or text — for the purposes of verifying the authenticity of the output or the identity or characteristics of its provenance, modifications, or conveyance.

Sec. 4. Ensuring the Safety and Security of AI Technology.

4.1. Developing Guidelines, Standards, and Best Practices for AI Safety and Security. (a) Within 270 days of the date of this order, to help ensure the development of safe, secure, and trustworthy AI systems, the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), in coordination with the Secretary of Energy, the Secretary of Homeland Security, and the heads of other relevant agencies as the Secretary of Commerce may deem appropriate, shall:

(i) Establish guidelines and best practices, with the aim of promoting consensus industry standards, for developing and deploying safe, secure, and trustworthy AI systems, including:

(A) developing a companion resource to the AI Risk Management Framework, NIST AI 100-1, for generative AI;

(B) developing a companion resource to the Secure Software Development Framework to incorporate secure development practices for generative AI and for dual-use foundation models; and

(C) launching an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm, such as in the areas of cybersecurity and biosecurity.

(ii) Establish appropriate guidelines (except for AI used as a component of a national security system), including appropriate procedures and processes, to enable developers of AI, especially of dual-use foundation models, to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems. These efforts shall include:

(A) coordinating or developing guidelines related to assessing and managing the safety, security, and trustworthiness of dual-use foundation models; and

(B) in coordination with the Secretary of Energy and the Director of the National Science Foundation (NSF), developing and helping to ensure the availability of testing environments, such as testbeds, to support the development of safe, secure, and trustworthy AI technologies, as well as to support the design, development, and deployment of associated PETs, consistent with section 9(b) of this order.

(b) Within 270 days of the date of this order, to understand and mitigate AI security risks, the Secretary of Energy, in coordination with the heads of other Sector Risk Management Agencies (SRMAs) as the Secretary of Energy may deem appropriate, shall develop and, to the extent permitted by law and available appropriations, implement a plan for developing the Department of Energy's AI model evaluation tools and AI testbeds. The Secretary shall undertake this work using existing solutions where possible, and shall develop these tools and AI testbeds to be capable of assessing near-term extrapolations of AI systems' capabilities. At a minimum, the Secretary shall develop tools to evaluate AI capabilities to generate outputs that may represent nuclear, nonproliferation, biological, chemical, critical infrastructure, and energy-security threats or hazards. The Secretary shall do this work solely for the purposes of guarding against these threats, and shall also develop model guardrails that reduce such risks. The Secretary shall, as appropriate, consult with private AI laboratories, academia, civil society, and third-party evaluators, and shall use existing solutions.

4.2. Ensuring Safe and Reliable AI. (a) Within 90 days of the date of this order, to ensure and verify the continuous availability of safe, reliable, and effective AI in accordance with the Defense Production Act, as amended, 50 U.S.C. 4501 *et seq*., including for the national defense and the protection of critical infrastructure, the Secretary of Commerce shall require:

(i) Companies developing or demonstrating an intent to develop potential dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records regarding the following:

(A) any ongoing or planned activities related to training, developing, or producing dual-use foundation models, including the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats;

(B) the ownership and possession of the model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights; and

(C) the results of any developed dual-use foundation model's performance in relevant AI red-team testing based on guidance developed by NIST pursuant to subsection 4.1(a)(ii) of this section, and a description of any associated measures the company has taken to meet safety objectives, such as mitigations to improve performance on these red-team tests and strengthen overall model security. Prior to the development of guidance on red-team testing standards by NIST pursuant to subsection 4.1(a)(ii) of this section, this description shall include the results of any red-team testing that the company has conducted relating to lowering the barrier to entry for the development, acquisition, and use of biological weapons by non-state actors; the discovery of software vulnerabilities and development of associated exploits; the use of software or tools to influence real or virtual events; the possibility for self-replication or propagation; and associated measures to meet safety objectives; and

(ii) Companies, individuals, or other organizations or entities that acquire, develop, or possess a potential large-scale computing cluster to report any such acquisition, development, or possession, including the existence and location of these clusters and the amount of total computing power available in each cluster.

(b) The Secretary of Commerce, in consultation with the Secretary of State, the Secretary of Defense, the Secretary of Energy, and the Director of National Intelligence, shall define, and thereafter update as needed on a regular basis, the set of technical conditions for models and computing clusters that would be subject to the reporting requirements of subsection 4.2(a) of this section. Until such technical conditions are defined, the Secretary shall require compliance with these reporting requirements for:

(i) any model that was trained using a quantity of computing power greater than 10^{26} integer or floating-point operations, or using primarily biological sequence data and using a quantity of computing power greater than 10^{23} integer or floating-point operations; and

(ii) any computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum computing capacity of 10^{20} integer or floating-point operations per second for training AI.

(c) Because I find that additional steps must be taken to deal with the national emergency related to significant malicious cyber-enabled activities declared in Executive Order 13694 of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities), as amended by Executive Order 13757 of December 28, 2016 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities), and further amended by Executive Order 13984, to address the use of United States Infrastructure as a Service (IaaS) Products by foreign malicious cyber actors, including to impose additional record-keeping obligations with respect to foreign transactions and to assist in the investigation of transactions involving foreign malicious cyber actors, I hereby direct the Secretary of Commerce, within 90 days of the date of this order, to:

(i) Propose regulations that require United States IaaS Providers to submit a report to the Secretary of Commerce when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity (a "training run"). Such reports shall include, at a minimum, the identity of the foreign person and the existence of any training run of an AI model meeting the criteria set forth in this section, or other criteria defined by the Secretary in regulations, as well as any additional information identified by the Secretary.

(ii) Include a requirement in the regulations proposed pursuant to subsection 4.2(c)(i) of this section that United States IaaS Providers prohibit any foreign reseller of their United States IaaS Product from providing those products unless such foreign reseller submits to the United States IaaS

Provider a report, which the United States IaaS Provider must provide to the Secretary of Commerce, detailing each instance in which a foreign person transacts with the foreign reseller to use the United States IaaS Product to conduct a training run described in subsection 4.2(c)(i) of this section. Such reports shall include, at a minimum, the information specified in subsection 4.2(c)(i) of this section as well as any additional information identified by the Secretary.

(iii) Determine the set of technical conditions for a large AI model to have potential capabilities that could be used in malicious cyber-enabled activity, and revise that determination as necessary and appropriate. Until the Secretary makes such a determination, a model shall be considered to have potential capabilities that could be used in malicious cyber-enabled activity if it requires a quantity of computing power greater than 10^{26} integer or floating-point operations and is trained on a computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum compute capacity of 10^{20} integer or floating-point operations per second for training AI.

(d) Within 180 days of the date of this order, pursuant to the finding set forth in subsection 4.2(c) of this section, the Secretary of Commerce shall propose regulations that require United States IaaS Providers to ensure that foreign resellers of United States IaaS Products verify the identity of any foreign person that obtains an IaaS account (account) from the foreign reseller. These regulations shall, at a minimum:

(i) Set forth the minimum standards that a United States IaaS Provider must require of foreign resellers of its United States IaaS Products to verify the identity of a foreign person who opens an account or maintains an existing account with a foreign reseller, including:

(A) the types of documentation and procedures that foreign resellers of United States IaaS Products must require to verify the identity of any foreign person acting as a lessee or sub-lessee of these products or services;

(B) records that foreign resellers of United States IaaS Products must securely maintain regarding a foreign person that obtains an account, including information establishing:

(1) the identity of such foreign person, including name and address;

(2) the means and source of payment (including any associated financial institution and other identifiers such as credit card number, account number, customer identifier, transaction identifiers, or virtual currency wallet or wallet address identifier);

(3) the electronic mail address and telephonic contact information used to verify a foreign person's identity; and

(4) the Internet Protocol addresses used for access or administration and the date and time of each such access or administrative action related to ongoing verification of such foreign person's ownership of such an account; and

(C) methods that foreign resellers of United States IaaS Products must implement to limit all third-party access to the information described in this subsection, except insofar as such access is otherwise consistent with this order and allowed under applicable law;

(ii) Take into consideration the types of accounts maintained by foreign resellers of United States IaaS Products, methods of opening an account, and types of identifying information available to accomplish the objectives of identifying foreign malicious cyber actors using any such products and avoiding the imposition of an undue burden on such resellers; and

(iii) Provide that the Secretary of Commerce, in accordance with such standards and procedures as the Secretary may delineate and in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, may exempt a United States IaaS Provider with respect to any specific foreign reseller of their United States IaaS Products, or with respect to any specific type of account or lessee, from the requirements of any regulation issued pursuant to this subsection. Such standards and procedures may include a finding by the Secretary that such foreign reseller, account, or lessee complies with security best practices to otherwise deter abuse of United States IaaS Products.

(e) The Secretary of Commerce is hereby authorized to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by the International Emergency Economic Powers Act, 50 U.S.C. 1701 *et seq.*, as may be necessary to carry out the purposes of subsections 4.2(c) and (d) of this section. Such actions may include a requirement that United States IaaS Providers require foreign resellers of United States IaaS Products to provide United States IaaS Providers verifications relative to those subsections.

4.3. Managing AI in Critical Infrastructure and in Cybersecurity. (a) To ensure the protection of critical
infrastructure, the following actions shall be taken:

(i) Within 90 days of the date of this order, and at least annually thereafter, the head of each agency with relevant regulatory authority over critical infrastructure and the heads of relevant SRMAs, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security for consideration of cross-sector risks, shall evaluate and provide to the Secretary of Homeland Security an assessment of potential risks related to the use of AI in critical infrastructure sectors involved, including ways in which deploying AI may make critical infrastructure systems more vulnerable to critical failures, physical attacks, and cyber attacks, and shall consider ways to mitigate these vulnerabilities. Independent regulatory agencies are encouraged, as they deem appropriate, to contribute to sector-specific risk assessments.

(ii) Within 150 days of the date of this order, the Secretary of the Treasury shall issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks.

(iii) Within 180 days of the date of this order, the Secretary of Homeland Security, in coordination with the Secretary of Commerce and with SRMAs and other regulators as determined by the Secretary of Homeland Security, shall incorporate as appropriate the AI Risk Management Framework, NIST AI 100-1, as well as other appropriate security guidance, into relevant safety and security guidelines for use by critical infrastructure owners and operators.

(iv) Within 240 days of the completion of the guidelines described in subsection 4.3(a)(iii) of this section, the Assistant to the President for National Security Affairs and the Director of OMB, in consultation with the Secretary of Homeland Security, shall coordinate work by the heads of agencies with authority over critical infrastructure to develop and take steps for the Federal Government to mandate such guidelines, or appropriate portions thereof, through regulatory or other appropriate action. Independent regulatory agencies are encouraged, as they deem appropriate, to consider whether to mandate guidance through regulatory action in their areas of authority and responsibility.

(v) The Secretary of Homeland Security shall establish an Artificial Intelligence Safety and Security Board as an advisory committee pursuant to section 871 of the Homeland Security Act of 2002 (Public Law 107-296). The Advisory Committee shall include AI experts from the private sector, academia, and government, as appropriate, and provide to the Secretary of Homeland Security and the Federal Government's critical infrastructure community advice, information, or recommendations for improving security, resilience, and incident response related to AI usage in critical infrastructure.

(b) To capitalize on AI's potential to improve United States cyber defenses:

(i) The Secretary of Defense shall carry out the actions described in subsections 4.3(b)(ii) and (iii) of this section for national security systems, and the Secretary of Homeland Security shall carry out these actions for non-national security systems. Each shall do so in consultation with the heads of other relevant agencies as the Secretary of Defense and the Secretary of Homeland Security may deem appropriate.

(ii) As set forth in subsection 4.3(b)(i) of this section, within 180 days of the date of this order, the Secretary of Defense and the Secretary of Homeland Security shall, consistent with applicable law, each develop plans for, conduct, and complete an operational pilot project to identify, develop, test, evaluate, and deploy AI capabilities, such as large-language models, to aid in the discovery and remediation of vulnerabilities in critical United States Government software, systems, and networks.

(iii) As set forth in subsection 4.3(b)(i) of this section, within 270 days of the date of this order, the Secretary of Defense and the Secretary of Homeland Security shall each provide a report to the Assistant to the President for National Security Affairs on the results of actions taken pursuant to the plans and operational pilot projects required by subsection 4.3(b)(ii) of this section, including a description of any vulnerabilities found and fixed through the development and deployment of AI capabilities and any lessons learned on how to identify, develop, test, evaluate, and deploy AI capabilities effectively for cyber defense.

4.4. Reducing Risks at the Intersection of AI and CBRN Threats. (a) To better understand and mitigate the risk of AI being misused to assist in the development or use of CBRN threats — with a particular focus on biological weapons — the following actions shall be taken:

(i) Within 180 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Energy and the Director of the Office of Science and Technology Policy (OSTP), shall evaluate the potential for AI to be misused to enable the development or production of CBRN threats, while also considering the benefits and application of AI to counter these threats, including, as appropriate, the results of work conducted under section 8(b) of this order. The Secretary of Homeland Security shall:

(A) consult with experts in AI and CBRN issues from the Department of Energy, private AI laboratories, academia, and third-party model evaluators, as appropriate, to evaluate AI model capabilities to present CBRN threats — for the sole purpose of guarding against those threats — as well as options for minimizing the risks of AI model misuse to generate or exacerbate those threats; and

(B) submit a report to the President that describes the progress of these efforts, including an assessment of the types of AI models that may present CBRN risks to the United States, and that makes recommendations for regulating or overseeing the training, deployment, publication, or use of these models, including requirements for safety evaluations and guardrails for mitigating potential threats to national security.

(ii) Within 120 days of the date of this order, the Secretary of Defense, in consultation with the Assistant to the President for National Security

Affairs and the Director of OSTP, shall enter into a contract with the National Academies of Sciences, Engineering, and Medicine to conduct — and submit to the Secretary of Defense, the Assistant to the President for National Security Affairs, the Director of the Office of Pandemic Preparedness and Response Policy, the Director of OSTP, and the Chair of the Chief Data Officer Council — a study that:

(A) assesses the ways in which AI can increase biosecurity risks, including risks from generative AI models trained on biological data, and makes recommendations on how to mitigate these risks;

(B) considers the national security implications of the use of data and datasets, especially those associated with pathogens and omics studies, that the United States Government hosts, generates, funds the creation of, or otherwise owns, for the training of generative AI models, and makes recommendations on how to mitigate the risks related to the use of these data and datasets;

(C) assesses the ways in which AI applied to biology can be used to reduce biosecurity risks, including recommendations on opportunities to coordinate data and high-performance computing resources; and

(D) considers additional concerns and opportunities at the intersection of AI and synthetic biology that the Secretary of Defense deems appropriate.

(b) To reduce the risk of misuse of synthetic nucleic acids, which could be substantially increased by AI's capabilities in this area, and improve biosecurity measures for the nucleic acid synthesis industry, the following actions shall be taken:

(i) Within 180 days of the date of this order, the Director of OSTP, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Health and Human Services (HHS), the Secretary of Energy, the Secretary of Homeland Security, the Director of National Intelligence, and the heads of other relevant agencies as the Director of OSTP may deem appropriate, shall establish a framework, incorporating, as appropriate, existing United States Government guidance, to encourage providers of synthetic nucleic acid sequences to implement comprehensive, scalable, and verifiable synthetic nucleic acid procurement screening mechanisms, including standards and recommended incentives. As part of this framework, the Director of OSTP shall:

(A) establish criteria and mechanisms for ongoing identification of biological sequences that could be used in a manner that would pose a risk to the national security of the United States; and

(B) determine standardized methodologies and tools for conducting and verifying the performance of sequence synthesis procurement screening, including customer screening approaches to support due diligence with respect to managing security risks posed by purchasers of biological sequences identified in subsection 4.4(b)(i)(A) of this section, and processes for the reporting of concerning activity to enforcement entities.

(ii) Within 180 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in coordination with the Director of OSTP, and in consultation with the Secretary of State, the Secretary of HHS, and the heads of other relevant agencies as the Secretary of Commerce may deem appropriate, shall initiate an effort to engage with industry and relevant stakeholders, informed by the framework developed under subsection 4.4(b)(i) of this section, to develop and refine for possible use by synthetic nucleic acid sequence providers:

(A) specifications for effective nucleic acid synthesis procurement screening;

(B) best practices, including security and access controls, for managing sequence-of-concern databases to support such screening;

(C) technical implementation guides for effective screening; and

(D) conformity-assessment best practices and mechanisms.

(iii) Within 180 days of the establishment of the framework pursuant to subsection 4.4(b)(i) of this section, all agencies that fund life-sciences research shall, as appropriate and consistent with applicable law, establish that, as a requirement of funding, synthetic nucleic acid procurement is conducted through providers or manufacturers that adhere to the framework, such as through an attestation from the provider or manufacturer. The Assistant to the President for National Security Affairs and the Director of OSTP shall coordinate the process of reviewing such funding requirements to facilitate consistency in implementation of the framework across funding agencies.

(iv)   In order to facilitate effective implementation of the measures described in subsections 4.4(b)(i)-(iii) of this section, the Secretary of Homeland Security, in consultation with the heads of other relevant agencies as the Secretary of Homeland Security may deem appropriate, shall:

(A) within 180 days of the establishment of the framework pursuant to subsection 4.4(b)(i) of this section, develop a framework to conduct structured evaluation and stress testing of nucleic acid synthesis procurement screening, including the systems developed in accordance with subsections 4.4(b)(i)-(ii) of this section and implemented by providers of synthetic nucleic acid sequences; and

(B) following development of the framework pursuant to subsection 4.4(b)(iv)(A) of this section, submit an annual report to the Assistant to the President for National Security Affairs, the Director of the Office of Pandemic Preparedness and Response Policy, and the Director of OSTP on any results of the activities conducted pursuant to subsection 4.4(b)(iv)(A) of this section, including recommendations, if any, on how to strengthen nucleic acid synthesis procurement screening, including customer screening systems.

4.5. Reducing the Risks Posed by Synthetic Content.

To foster capabilities for identifying and labeling synthetic content produced by AI systems, and to establish the authenticity and provenance of digital content, both synthetic and not synthetic, produced by the Federal Government or on its behalf:

(a) Within 240 days of the date of this order, the Secretary of Commerce, in consultation with the heads of other relevant agencies as the Secretary of Commerce may deem appropriate, shall submit a report to the Director of OMB and the Assistant to the President for National Security Affairs identifying the existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, for:

(i) authenticating content and tracking its provenance;

(ii) labeling synthetic content, such as using watermarking;

(iii) detecting synthetic content;

(iv) preventing generative AI from producing child sexual abuse material or producing non-consensual intimate imagery of real individuals (to include intimate digital depictions of the body or body parts of an identifiable individual);

(v) testing software used for the above purposes; and

(vi) auditing and maintaining synthetic content.

(b) Within 180 days of submitting the report required under subsection 4.5(a) of this section, and updated periodically thereafter, the Secretary of Commerce, in coordination with the Director of OMB, shall develop guidance regarding the existing tools and practices for digital content authentication and synthetic content detection measures. The guidance shall include measures for the purposes listed in subsection 4.5(a) of this section.

(c) Within 180 days of the development of the guidance required under subsection 4.5(b) of this section, and updated periodically thereafter, the Director of OMB, in consultation with the Secretary of State; the Secretary of Defense; the Attorney General; the Secretary of Commerce, acting through the Director of NIST; the Secretary of Homeland Security; the Director of National Intelligence; and the heads of other agencies that the Director of OMB deems appropriate, shall — for the purpose of strengthening public confidence in the integrity of official United States Government digital content — issue guidance to agencies for labeling and authenticating such content that they produce or publish.

(d) The Federal Acquisition Regulatory Council shall, as appropriate and consistent with applicable law, consider amending the Federal Acquisition Regulation to take into account the guidance established under subsection 4.5 of this section.

4.6. Soliciting Input on Dual-Use Foundation Models with Widely Available Model Weights. When the weights for a dual-use foundation model are widely available — such as when they are publicly posted on the Internet — there can be substantial benefits to innovation, but also substantial security risks, such as the removal of safeguards within the model. To address the risks and potential benefits of dual-use foundation models with widely available weights, within 270 days of the date of this order, the Secretary of Commerce, acting through the Assistant Secretary of Commerce for Communications and Information, and in consultation with the Secretary of State, shall:

(a) solicit input from the private sector, academia, civil society, and other stakeholders through a public consultation process on potential risks, benefits, other implications, and appropriate policy and regulatory approaches related to dual-use foundation models for which the model weights are widely available, including:

(i) risks associated with actors fine-tuning dual-use foundation models for which the model weights are widely available or removing those models' safeguards;

(ii) benefits to AI innovation and research, including research into AI safety and risk management, of dual-use foundation models for which the model weights are widely available; and

(iii) potential voluntary, regulatory, and international mechanisms to manage the risks and maximize the benefits of dual-use foundation models for which the model weights are widely available; and

(b) based on input from the process described in subsection 4.6(a) of this section, and in consultation with the heads of other relevant agencies as the

Secretary of Commerce deems appropriate, submit a report to the President on the potential benefits, risks, and implications of dual-use foundation models for which the model weights are widely available, as well as policy and regulatory recommendations pertaining to those models.

4.7. Promoting Safe Release and Preventing the Malicious Use of Federal Data for AI Training.To improve public data access and manage security risks, and consistent with the objectives of the Open, Public, Electronic, and Necessary Government Data Act (title II of Public Law 115-435) to expand public access to Federal data assets in a machine-readable format while also taking into account security considerations, including the risk that information in an individual data asset in isolation does not pose a security risk but, when combined with other available information, may pose such a risk:

(a) within 270 days of the date of this order, the Chief Data Officer Council, in consultation with the Secretary of Defense, the Secretary of Commerce, the Secretary of Energy, the Secretary of Homeland Security, and the Director of National Intelligence, shall develop initial guidelines for performing security reviews, including reviews to identify and manage the potential security risks of releasing Federal data that could aid in the development of CBRN weapons as well as the development of autonomous offensive cyber capabilities, while also providing public access to Federal Government data in line with the goals stated in the Open, Public, Electronic, and Necessary Government Data Act (title II of Public Law 115-435); and

(b) within 180 days of the development of the initial guidelines required by subsection 4.7(a) of this section, agencies shall conduct a security review of all data assets in the comprehensive data inventory required under 44 U.S.C. 3511(a)(1) and (2)(B) and shall take steps, as appropriate and consistent with applicable law, to address the highest-priority potential security risks that releasing that data could raise with respect to CBRN weapons, such as the ways in which that data could be used to train AI systems.

4.8. Directing the Development of a National Security Memorandum. To develop a coordinated executive branch approach to managing AI's security risks, the Assistant to the President for National Security Affairs and the Assistant to the President and Deputy Chief of Staff for Policy shall oversee an interagency process with the purpose of, within 270 days of the date of this order, developing and submitting a proposed National Security Memorandum on AI to the President. The memorandum shall address the governance of AI used as a component of a national security system or for military and intelligence purposes. The memorandum shall take into account current efforts to govern the development and use of AI for national security systems. The memorandum shall outline actions for the Department of Defense, the Department of State, other relevant agencies, and the Intelligence Community to address the national security risks and potential benefits posed by AI. In particular, the memorandum shall:

(a) provide guidance to the Department of Defense, other relevant agencies, and the Intelligence Community on the continued adoption of AI capabilities to advance the United States national security mission, including through directing specific AI assurance and risk-management practices for national security uses of AI that may affect the rights or safety of United States persons and, in appropriate contexts, non-United States persons; and

(b) direct continued actions, as appropriate and consistent with applicable law, to address the potential use of AI systems by adversaries and other foreign actors in ways that threaten the capabilities or objectives of the Department of Defense or the Intelligence Community, or that otherwise pose risks to the security of the United States or its allies and partners.

Sec. 5. Promoting Innovation and Competition.

5.1. Attracting AI Talent to the United States. (a) Within 90 days of the date of this order, to attract and retain talent in AI and other critical and emerging technologies in the United States economy, the Secretary of State and the Secretary of Homeland Security shall take appropriate steps to:

(i) streamline processing times of visa petitions and applications, including by ensuring timely availability of visa appointments, for noncitizens who seek to travel to the United States to work on, study, or conduct research in AI or other critical and emerging technologies; and

(ii) facilitate continued availability of visa appointments in sufficient volume for applicants with expertise in AI or other critical and emerging technologies.

(b) Within 120 days of the date of this order, the Secretary of State shall:

(i) consider initiating a rulemaking to establish new criteria to designate countries and skills on the Department of State's Exchange Visitor Skills List as it relates to the 2-year foreign residence requirement for certain J-1 nonimmigrants, including those skills that are critical to the United States;

(ii) consider publishing updates to the 2009 Revised Exchange Visitor Skills List (74 FR 20108); and

(iii) consider implementing a domestic visa renewal program under 22 C.F.R. 41.111(b) to facilitate the ability of qualified applicants, including highly skilled talent in AI and critical and emerging technologies, to continue their work in the United States without unnecessary interruption.

(c) Within 180 days of the date of this order, the Secretary of State shall:

(i) consider initiating a rulemaking to expand the categories of nonimmigrants who qualify for the domestic visa renewal program covered under 22 C.F.R. 41.111(b) to include academic J-1 research scholars and F-1 students in science, technology, engineering, and mathematics (STEM); and

(ii) establish, to the extent permitted by law and available appropriations, a program to identify and attract top talent in AI and other critical and emerging technologies at universities, research institutions, and the private sector overseas, and to establish and increase connections with that talent to educate them on opportunities and resources for research and employment in the United States, including overseas educational components to inform top STEM talent of nonimmigrant and immigrant visa options and potential expedited adjudication of their visa petitions and applications.

(d) Within 180 days of the date of this order, the Secretary of Homeland Security shall:

(i) review and initiate any policy changes the Secretary determines necessary and appropriate to clarify and modernize immigration pathways for experts in AI and other critical and emerging technologies, including O-1A and EB-1 noncitizens of extraordinary ability; EB-2 advanced-degree holders and noncitizens of exceptional ability; and startup founders in AI and other critical and emerging technologies using the International Entrepreneur Rule; and

(ii) continue its rulemaking process to modernize the H-1B program and enhance its integrity and usage, including by experts in AI and other critical and emerging technologies, and consider initiating a rulemaking to enhance the process for noncitizens, including experts in AI and other critical and emerging technologies and their spouses, dependents, and children, to adjust their status to lawful permanent resident.

(e) Within 45 days of the date of this order, for purposes of considering updates to the "Schedule A" list of occupations, 20 C.F.R. 656.5, the Secretary of Labor shall publish a request for information (RFI) to solicit public input, including from industry and worker-advocate communities, identifying AI and other STEM-related occupations, as well as additional occupations across the economy, for which there is an insufficient number of ready, willing, able, and qualified United States workers.

(f) The Secretary of State and the Secretary of Homeland Security shall, consistent with applicable law and implementing regulations, use their discretionary authorities to support and attract foreign nationals with special skills in AI and other critical and emerging technologies seeking to work, study, or conduct research in the United States.

(g) Within 120 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of OSTP, shall develop and publish informational resources to better attract and retain experts in AI and other critical and emerging technologies, including:

(i) a clear and comprehensive guide for experts in AI and other critical and emerging technologies to understand their options for working in the United States, to be published in multiple relevant languages on AI.gov; and

(ii) a public report with relevant data on applications, petitions, approvals, and other key indicators of how experts in AI and other critical and emerging technologies have utilized the immigration system through the end of Fiscal Year 2023.

5.2. Promoting Innovation. (a) To develop and strengthen public-private partnerships for advancing innovation, commercialization, and risk-mitigation methods for AI, and to help promote safe, responsible, fair, privacy-protecting, and trustworthy AI systems, the Director of NSF shall take the following steps:

(i) Within 90 days of the date of this order, in coordination with the heads of agencies that the Director of NSF deems appropriate, launch a pilot program implementing the National AI Research Resource (NAIRR), consistent with past recommendations of the NAIRR Task Force. The program shall pursue the infrastructure, governance mechanisms, and user interfaces to pilot an initial integration of distributed computational, data, model, and training resources to be made available to the research community in support of AI-related research and development. The Director of NSF shall identify Federal and private sector computational, data, software, and training resources appropriate for inclusion in the NAIRR pilot program. To assist with such work, within 45 days of the date of this order, the heads of agencies whom the Director of NSF identifies for coordination pursuant to this subsection shall each submit to the Director of NSF a report identifying the agency resources that could be developed and integrated into such a pilot program. These reports shall include a description of such resources, including their current status and availability; their format, structure, or technical specifications; associated agency expertise that will be provided; and the benefits and risks associated with their inclusion in the NAIRR pilot program. The heads of independent regulatory agencies are encouraged to take similar steps, as they deem appropriate.

(ii) Within 150 days of the date of this order, fund and launch at least one NSF Regional Innovation Engine that prioritizes AI-related work, such as AI-related research, societal, or workforce needs.

(iii) Within 540 days of the date of this order, establish at least four new National AI Research Institutes, in addition to the 25 currently funded as of the date of this order.

(b) Within 120 days of the date of this order, to support activities involving high-performance and data-intensive computing, the Secretary of Energy, in coordination with the Director of NSF, shall, in a manner consistent with applicable law and available appropriations, establish a pilot program to enhance existing successful training programs for scientists, with the goal of training 500 new researchers by 2025 capable of meeting the rising demand for AI talent.

(c) To promote innovation and clarify issues related to AI and inventorship of patentable subject matter, the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office (USPTO Director) shall:

(i) within 120 days of the date of this order, publish guidance to USPTO patent examiners and applicants addressing inventorship and the use of AI, including generative AI, in the inventive process, including illustrative examples in which AI systems play different roles in inventive processes and how, in each example, inventorship issues ought to be analyzed;

(ii) subsequently, within 270 days of the date of this order, issue additional guidance to USPTO patent examiners and applicants to address other considerations at the intersection of AI and IP, which could include, as the USPTO Director deems necessary, updated guidance on patent eligibility to address innovation in AI and critical and emerging technologies; and

(iii) within 270 days of the date of this order or 180 days after the United States Copyright Office of the Library of Congress publishes its forthcoming AI study that will address copyright issues raised by AI, whichever comes later, consult with the Director of the United States Copyright Office and issue recommendations to the President on potential executive actions relating to copyright and AI. The recommendations shall address any copyright and related issues discussed in the United States Copyright Office's study, including the scope of protection for works produced using AI and the treatment of copyrighted works in AI training.

(d) Within 180 days of the date of this order, to assist developers of AI in combatting AI-related IP risks, the Secretary of Homeland Security, acting through the Director of the National Intellectual Property Rights Coordination Center, and in consultation with the Attorney General, shall develop a training, analysis, and evaluation program to mitigate AI-related IP risks. Such a program shall:

(i) include appropriate personnel dedicated to collecting and analyzing reports of AI-related IP theft, investigating such incidents with implications for national security, and, where appropriate and consistent with applicable law, pursuing related enforcement actions;

(ii) implement a policy of sharing information and coordinating on such work, as appropriate and consistent with applicable law, with the Federal Bureau of Investigation; United States Customs and Border Protection; other agencies; State and local agencies; and appropriate international organizations, including through work-sharing agreements;

(iii) develop guidance and other appropriate resources to assist private sector actors with mitigating the risks of AI-related IP theft;

(iv) share information and best practices with AI developers and law enforcement personnel to identify incidents, inform stakeholders of current legal requirements, and evaluate AI systems for IP law violations, as well as develop mitigation strategies and resources; and

(v) assist the Intellectual Property Enforcement Coordinator in updating the Intellectual Property Enforcement Coordinator Joint Strategic Plan on Intellectual Property Enforcement to address AI-related issues.

(e) To advance responsible AI innovation by a wide range of healthcare technology developers that promotes the welfare of patients and workers in the healthcare sector, the Secretary of HHS shall identify and, as appropriate and consistent with applicable law and the activities directed in section 8 of this order, prioritize grantmaking and other awards, as well as undertake related efforts, to support responsible AI development and use, including:

(i) collaborating with appropriate private sector actors through HHS programs that may support the advancement of AI-enabled tools that develop personalized immune-response profiles for patients, consistent with section 4 of this order;

(ii) prioritizing the allocation of 2024 Leading Edge Acceleration Project cooperative agreement awards to initiatives that explore ways to improve healthcare-data quality to support the responsible development of

AI tools for clinical care, real-world-evidence programs, population health, public health, and related research; and

(iii) accelerating grants awarded through the National Institutes of Health Artificial Intelligence/Machine Learning Consortium to Advance Health Equity and Researcher Diversity (AIM-AHEAD) program and showcasing current AIM-AHEAD activities in underserved communities.

(f) To advance the development of AI systems that improve the quality of veterans' healthcare, and in order to support small businesses' innovative capacity, the Secretary of Veterans Affairs shall:

(i) within 365 days of the date of this order, host two 3-month nationwide AI Tech Sprint competitions; and

(ii) as part of the AI Tech Sprint competitions and in collaboration with appropriate partners, provide participants access to technical assistance, mentorship opportunities, individualized expert feedback on products under development, potential contract opportunities, and other programming and resources.

(g) Within 180 days of the date of this order, to support the goal of strengthening our Nation's resilience against climate change impacts and building an equitable clean energy economy for the future, the Secretary of Energy, in consultation with the Chair of the Federal Energy Regulatory Commission, the Director of OSTP, the Chair of the Council on Environmental Quality, the Assistant to the President and National Climate Advisor, and the heads of other relevant agencies as the Secretary of Energy may deem appropriate, shall:

(i) issue a public report describing the potential for AI to improve planning, permitting, investment, and operations for electric grid infrastructure and to enable the provision of clean, affordable, reliable, resilient, and secure electric power to all Americans;

(ii) develop tools that facilitate building foundation models useful for basic and applied science, including models that streamline permitting and environmental reviews while improving environmental and social outcomes;

(iii) collaborate, as appropriate, with private sector organizations and members of academia to support development of AI tools to mitigate climate change risks;

(iv) take steps to expand partnerships with industry, academia, other agencies, and international allies and partners to utilize the Department of Energy's computing capabilities and AI testbeds to build foundation models that support new applications in science and energy, and for national security, including partnerships that increase community preparedness for climate-related risks, enable clean-energy deployment (including addressing delays in permitting reviews), and enhance grid reliability and resilience; and

(v) establish an office to coordinate development of AI and other critical and emerging technologies across Department of Energy programs and the 17 National Laboratories.

(h) Within 180 days of the date of this order, to understand AI's implications for scientific research, the President's Council of Advisors on Science and Technology shall submit to the President and make publicly available a report on the potential role of AI, especially given recent developments in AI, in research aimed at tackling major societal and global challenges. The report shall include a discussion of issues that may hinder the effective use of AI in research and practices needed to ensure that AI is used responsibly for research.

5.3. Promoting Competition. (a) The head of each agency developing policies and regulations related to AI shall use their authorities, as appropriate and consistent with applicable law, to promote competition in AI and related technologies, as well as in other markets. Such actions include addressing risks arising from concentrated control of key inputs, taking steps to stop unlawful collusion and prevent dominant firms from disadvantaging competitors, and working to provide new opportunities for small businesses and entrepreneurs. In particular, the Federal Trade Commission is encouraged to consider, as it deems appropriate, whether to exercise the Commission's existing authorities, including its rulemaking authority under the Federal Trade Commission Act, 15 U.S.C. 41 *et seq.*, to ensure fair competition in the AI marketplace and to ensure that consumers and workers are protected from harms that may be enabled by the use of AI.

(b) To promote competition and innovation in the semiconductor industry, recognizing that semiconductors power AI technologies and that their availability is critical to AI competition, the Secretary of Commerce shall, in implementing division A of Public Law 117-167, known as the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022, promote competition by:

(i) implementing a flexible membership structure for the National Semiconductor Technology Center that attracts all parts of the semiconductor and microelectronics ecosystem, including startups and small firms;

(ii) implementing mentorship programs to increase interest and participation in the semiconductor industry, including from workers in underserved communities;

(iii) increasing, where appropriate and to the extent permitted by law, the availability of resources to startups and small businesses, including:

(A) funding for physical assets, such as specialty equipment or facilities, to which startups and small businesses may not otherwise have access;

(B) datasets — potentially including test and performance data — collected, aggregated, or shared by CHIPS research and development programs;

(C) workforce development programs;

(D) design and process technology, as well as IP, as appropriate; and

(E) other resources, including technical and intellectual property assistance, that could accelerate commercialization of new technologies by startups and small businesses, as appropriate; and

(iv) considering the inclusion, to the maximum extent possible, and as consistent with applicable law, of competition-increasing measures in notices of funding availability for commercial research-and-development facilities focused on semiconductors, including measures that increase access to facility capacity for startups or small firms developing semiconductors used to power AI technologies.

(c) To support small businesses innovating and commercializing AI, as well as in responsibly adopting and deploying AI, the Administrator of the Small Business Administration shall:

(i) prioritize the allocation of Regional Innovation Cluster program funding for clusters that support planning activities related to the establishment of one or more Small Business AI Innovation and Commercialization Institutes that provide support, technical assistance, and other resources to small businesses seeking to innovate, commercialize, scale, or otherwise advance the development of AI;

(ii) prioritize the allocation of up to $2 million in Growth Accelerator Fund Competition bonus prize funds for accelerators that support the incorporation or expansion of AI-related curricula, training, and technical assistance, or other AI-related resources within their programming; and

(iii) assess the extent to which the eligibility criteria of existing programs, including the State Trade Expansion Program, Technical and Business Assistance funding, and capital-access programs — such as the 7(a) loan program, 504 loan program, and Small Business Investment Company (SBIC) program — support appropriate expenses by small businesses related to the adoption of AI and, if feasible and appropriate, revise eligibility criteria to improve support for these expenses.

(d) The Administrator of the Small Business Administration, in coordination with resource partners, shall conduct outreach regarding, and raise awareness of, opportunities for small businesses to use capital-access programs described in subsection 5.3(c) of this section for eligible AI-related purposes, and for eligible investment funds with AI-related expertise — particularly those seeking to serve or with experience serving underserved communities — to apply for an SBIC license.

Sec. 6. Supporting Workers.(a) To advance the Government's understanding of AI's implications for workers, the following actions shall be taken within 180 days of the date of this order:

(i) The Chairman of the Council of Economic Advisers shall prepare and submit a report to the President on the labor-market effects of AI.

(ii) To evaluate necessary steps for the Federal Government to address AI-related workforce disruptions, the Secretary of Labor shall submit to the President a report analyzing the abilities of agencies to support workers displaced by the adoption of AI and other technological advancements. The report shall, at a minimum:

(A) assess how current or formerly operational Federal programs designed to assist workers facing job disruptions — including unemployment insurance and programs authorized by the Workforce Innovation and Opportunity Act (Public Law 113-128) — could be used to respond to possible future AI-related disruptions; and

(B) identify options, including potential legislative measures, to strengthen or develop additional Federal support for workers displaced by AI and, in consultation with the Secretary of Commerce and the Secretary of Education, strengthen and expand education and training opportunities that provide individuals pathways to occupations related to AI.

(b) To help ensure that AI deployed in the workplace advances employees' well-being:

(i) The Secretary of Labor shall, within 180 days of the date of this order and in consultation with other agencies and with outside entities, including labor unions and workers, as the Secretary of Labor deems appropriate, 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. The principles and best practices shall include specific steps for employers to take with regard to AI, and shall cover, at a minimum:

(A) job-displacement risks and career opportunities related to AI, including effects on job skills and evaluation of applicants and workers;

(B) labor standards and job quality, including issues related to the equity, protected-activity, compensation, health, and safety implications of AI in the workplace; and

(C) implications for workers of employers' AI-related collection and use of data about them, including transparency, engagement, management, and activity protected under worker-protection laws.

(ii) After principles and best practices are developed pursuant to subsection (b)(i) of this section, the heads of agencies shall consider, in consultation with the Secretary of Labor, encouraging the adoption of these guidelines in their programs to the extent appropriate for each program and consistent with applicable law.

(iii) To support employees whose work is monitored or augmented by AI in being compensated appropriately for all of their work time, the Secretary of Labor shall issue guidance to make clear that employers that deploy AI to monitor or augment employees' work must continue to comply with protections that ensure that workers are compensated for their hours worked, as defined under the Fair Labor Standards Act of 1938, 29 U.S.C. 201 *et seq.*, and other legal requirements.

(c) To foster a diverse AI-ready workforce, the Director of NSF shall prioritize available resources to support AI-related education and AI-related workforce development through existing programs. The Director shall additionally consult with agencies, as appropriate, to identify further opportunities for agencies to allocate resources for those purposes. The actions by the Director shall use appropriate fellowship programs and awards for these purposes.

Sec. 7. Advancing Equity and Civil Rights.

7.1. Strengthening AI and Civil Rights in the Criminal Justice System. (a) To address unlawful discrimination and other harms that may be exacerbated by AI, the Attorney General shall:

(i) consistent with Executive Order 12250 of November 2, 1980 (Leadership and Coordination of Nondiscrimination Laws), Executive Order 14091, and 28 C.F.R. 0.50-51, coordinate with and support agencies in their implementation and enforcement of existing Federal laws to address civil rights and civil liberties violations and discrimination related to AI;

(ii) direct the Assistant Attorney General in charge of the Civil Rights Division to convene, within 90 days of the date of this order, a meeting of the heads of Federal civil rights offices — for which meeting the heads of civil rights offices within independent regulatory agencies will be encouraged to join — to discuss comprehensive use of their respective authorities and offices to: prevent and address discrimination in the use of automated systems, including algorithmic discrimination; increase coordination between the Department of Justice's Civil Rights Division and Federal civil rights offices concerning issues related to AI and algorithmic discrimination; improve external stakeholder engagement to promote public awareness of potential discriminatory uses and effects of AI; and develop, as appropriate, additional training, technical assistance, guidance, or other resources; and

(iii) consider providing, as appropriate and consistent with applicable law, guidance, technical assistance, and training to State, local, Tribal, and territorial investigators and prosecutors on best practices for investigating and prosecuting civil rights violations and discrimination related to automated systems, including AI.

(b) To promote the equitable treatment of individuals and adhere to the Federal Government's fundamental obligation to ensure fair and impartial justice for all, with respect to the use of AI in the criminal justice system, the Attorney General shall, in consultation with the Secretary of Homeland Security and the Director of OSTP:

(i) within 365 days of the date of this order, submit to the President a report that addresses the use of AI in the criminal justice system, including any use in:

(A) sentencing;

(B) parole, supervised release, and probation;

(C) bail, pretrial release, and pretrial detention;

(D) risk assessments, including pretrial, earned time, and early release or transfer to home-confinement determinations;

(E) police surveillance;

(F) crime forecasting and predictive policing, including the ingestion of historical crime data into AI systems to predict high-density "hot spots";

(G) prison-management tools; and

(H) forensic analysis;

(ii) within the report set forth in subsection 7.1(b)(i) of this section:

(A) identify areas where AI can enhance law enforcement efficiency and accuracy, consistent with protections for privacy, civil rights, and civil liberties; and

(B) recommend best practices for law enforcement agencies, including safeguards and appropriate use limits for AI, to address the concerns set forth in section 13(e)(i) of Executive Order 14074 as well as the best practices and the guidelines set forth in section 13(e)(iii) of Executive Order 14074; and

(iii) supplement the report set forth in subsection 7.1(b)(i) of this section as appropriate with recommendations to the President, including with respect to requests for necessary legislation.

(c) To advance the presence of relevant technical experts and expertise (such as machine-learning engineers, software and infrastructure engineering, data privacy experts, data scientists, and user experience researchers) among law enforcement professionals:

(i) The interagency working group created pursuant to section 3 of Executive Order 14074 shall, within 180 days of the date of this order, identify and share best practices for recruiting and hiring law enforcement professionals who have the technical skills mentioned in subsection 7.1(c) of this section, and for training law enforcement professionals about responsible application of AI.

(ii) Within 270 days of the date of this order, the Attorney General shall, in consultation with the Secretary of Homeland Security, consider those best practices and the guidance developed under section 3(d) of Executive Order 14074 and, if necessary, develop additional general recommendations for State, local, Tribal, and territorial law enforcement agencies and criminal justice agencies seeking to recruit, hire, train, promote, and retain highly qualified and service-oriented officers and staff with relevant technical knowledge. In considering this guidance, the Attorney General shall consult with State, local, Tribal, and territorial law enforcement agencies, as appropriate.

(iii) Within 365 days of the date of this order, the Attorney General shall review the work conducted pursuant to section 2(b) of Executive Order 14074 and, if appropriate, reassess the existing capacity to investigate law enforcement deprivation of rights under color of law resulting from the use of AI, including through improving and increasing training of Federal law enforcement officers, their supervisors, and Federal prosecutors on how to investigate and prosecute cases related to AI involving the deprivation of rights under color of law pursuant to 18 U.S.C. 242.

7.2. Protecting Civil Rights Related to Government Benefits and Programs. (a) To advance equity and civil rights, consistent with the directives of Executive Order 14091, and in addition to complying with the guidance on Federal Government use of AI issued pursuant to section 10.1(b) of this order, agencies shall use their respective civil rights and civil liberties offices and authorities — as appropriate and consistent with applicable law — to prevent and address unlawful discrimination and other harms that result from uses of AI in Federal Government programs and benefits administration. This directive does not apply to agencies' civil or criminal enforcement authorities. Agencies shall consider opportunities to ensure that their respective civil rights and civil liberties offices are appropriately consulted on agency decisions regarding the design, development, acquisition, and use of AI in Federal Government programs and benefits administration. To further these objectives, agencies shall also consider opportunities to increase coordination, communication, and engagement about AI as appropriate with community-based organizations; civil-rights and civil-liberties organizations; academic institutions; industry; State, local, Tribal, and territorial governments; and other stakeholders.

(b) To promote equitable administration of public benefits:

(i) The Secretary of HHS shall, within 180 days of the date of this order and in consultation with relevant agencies, publish a plan, informed by the guidance issued pursuant to section 10.1(b) of this order, addressing the use of automated or algorithmic systems in the implementation by States and localities of public benefits and services administered by the Secretary, such as to promote: assessment of access to benefits by qualified recipients; notice to recipients about the presence of such systems; regular evaluation to detect unjust denials; processes to retain appropriate levels of discretion of expert agency staff; processes to appeal denials to human reviewers; and analysis of whether algorithmic systems in use by benefit programs achieve equitable and just outcomes.

(ii) The Secretary of Agriculture shall, within 180 days of the date of this order and as informed by the guidance issued pursuant to section 10.1(b) of this order, issue guidance to State, local, Tribal, and territorial public-benefits administrators on the use of automated or algorithmic systems in implementing benefits or in providing customer support for benefit programs administered by the Secretary, to ensure that programs using those systems:

(A) maximize program access for eligible recipients;

(B) employ automated or algorithmic systems in a manner consistent with any requirements for using merit systems personnel in public-benefits programs;

(C) identify instances in which reliance on automated or algorithmic systems would require notification by the State, local, Tribal, or territorial government to the Secretary;

(D) identify instances when applicants and participants can appeal benefit determinations to a human reviewer for reconsideration and can receive other customer support from a human being;

(E) enable auditing and, if necessary, remediation of the logic used to arrive at an individual decision or determination to facilitate the evaluation of appeals; and

(F) enable the analysis of whether algorithmic systems in use by benefit programs achieve equitable outcomes.

7.3. Strengthening AI and Civil Rights in the Broader Economy. (a) Within 365 days of the date of this order, to prevent unlawful discrimination from AI used for hiring, the Secretary of Labor shall publish guidance for Federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems.

(b) To address discrimination and biases against protected groups in housing markets and consumer financial markets, the Director of the Federal Housing Finance Agency and the Director of the Consumer Financial Protection Bureau are encouraged to consider using their authorities, as they deem appropriate, to require their respective regulated entities, where possible, to use appropriate methodologies including AI tools to ensure compliance with Federal law and:

(i) evaluate their underwriting models for bias or disparities affecting protected groups; and

(ii) evaluate automated collateral-valuation and appraisal processes in ways that minimize bias.

(c) Within 180 days of the date of this order, to combat unlawful discrimination enabled by automated or algorithmic tools used to make decisions about access to housing and in other real estate-related transactions, the Secretary of Housing and Urban Development shall, and the Director of the Consumer Financial Protection Bureau is encouraged to, issue additional guidance:

(i) addressing the use of tenant screening systems in ways that may violate the Fair Housing Act (Public Law 90-284), the Fair Credit Reporting Act (Public Law 91-508), or other relevant Federal laws, including how the use of data, such as criminal records, eviction records, and credit information, can lead to discriminatory outcomes in violation of Federal law; and

(ii) addressing how the Fair Housing Act, the Consumer Financial Protection Act of 2010 (title X of Public Law 111-203), or the Equal Credit Opportunity Act (Public Law 93-495) apply to the advertising of housing, credit, and other real estate-related transactions through digital platforms, including those that use algorithms to facilitate advertising delivery, as well as on best practices to avoid violations of Federal law.

(d) To help ensure that people with disabilities benefit from AI's promise while being protected from its risks, including unequal treatment from the use of biometric data like gaze direction, eye tracking, gait analysis, and hand motions, the Architectural and Transportation Barriers Compliance Board is encouraged, as it deems appropriate, to solicit public participation and conduct community engagement; to issue technical assistance and recommendations on the risks and benefits of AI in using biometric data as an input; and to provide people with disabilities access to information and communication technology and transportation services.

Sec. 8. Protecting Consumers, Patients, Passengers, and Students. (a) Independent regulatory agencies are encouraged, as they deem appropriate, to consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI, including risks to financial stability, and to consider rulemaking, as well as emphasizing or clarifying where existing regulations and guidance apply to AI, including clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use, and emphasizing or clarifying requirements and expectations related to the transparency of AI models and regulated entities' ability to explain their use of AI models.

(b) To help ensure the safe, responsible deployment and use of AI in the healthcare, public-health, and human-services sectors:

(i) Within 90 days of the date of this order, the Secretary of HHS shall, in consultation with the Secretary of Defense and the Secretary of Veterans Affairs, establish an HHS AI Task Force that shall, within 365 days of its creation, develop a strategic plan that includes policies and frameworks — possibly including regulatory action, as appropriate — on responsible deployment and use of AI and AI-enabled technologies in the health and human services sector (including research and discovery, drug and device safety, healthcare delivery and financing, and public health), and identify appropriate guidance and resources to promote that deployment, including in the following areas:

(A) development, maintenance, and use of predictive and generative AI-enabled technologies in healthcare delivery and financing — including quality measurement, performance improvement, program integrity, benefits administration, and patient experience — taking into account considerations such as appropriate human oversight of the application of AI-generated output;

(B) long-term safety and real-world performance monitoring of AI-enabled technologies in the health and human services sector, including clinically relevant or significant modifications and performance across population groups, with a means to communicate product updates to regulators, developers, and users;

(C) incorporation of equity principles in AI-enabled technologies used in the health and human services sector, using disaggregated data on affected populations and representative population data sets when developing new models, monitoring algorithmic performance against discrimination and bias in existing models, and helping to identify and mitigate discrimination and bias in current systems;

(D) incorporation of safety, privacy, and security standards into the software-development lifecycle for protection of personally identifiable information, including measures to address AI-enhanced cybersecurity threats in the health and human services sector;

(E) development, maintenance, and availability of documentation to help users determine appropriate and safe uses of AI in local settings in the health and human services sector;

(F) work to be done with State, local, Tribal, and territorial health and human services agencies to advance positive use cases and best practices for use of AI in local settings; and

(G) identification of uses of AI to promote workplace efficiency and satisfaction in the health and human services sector, including reducing administrative burdens.

(ii) Within 180 days of the date of this order, the Secretary of HHS shall direct HHS components, as the Secretary of HHS deems appropriate, to develop a strategy, in consultation with relevant agencies, to determine whether AI-enabled technologies in the health and human services sector maintain appropriate levels of quality, including, as appropriate, in the areas described in subsection (b)(i) of this section. This work shall include the development of AI assurance policy — to evaluate important aspects of the performance of AI-enabled healthcare tools — and infrastructure needs for enabling pre-market assessment and post-market oversight of AI-enabled healthcare-technology algorithmic system performance against real-world data.

(iii) Within 180 days of the date of this order, the Secretary of HHS shall, in consultation with relevant agencies as the Secretary of HHS deems appropriate, consider appropriate actions to advance the prompt understanding of, and compliance with, Federal nondiscrimination laws by health and human services providers that receive Federal financial assistance, as well as how those laws relate to AI. Such actions may include:

(A) convening and providing technical assistance to health and human services providers and payers about their obligations under Federal nondiscrimination and privacy laws as they relate to AI and the potential consequences of noncompliance; and

(B) issuing guidance, or taking other action as appropriate, in response to any complaints or other reports of noncompliance with Federal nondiscrimination and privacy laws as they relate to AI.

(iv) Within 365 days of the date of this order, the Secretary of HHS shall, in consultation with the Secretary of Defense and the Secretary of Veterans Affairs, establish an AI safety program that, in partnership with voluntary federally listed Patient Safety Organizations:

(A) establishes a common framework for approaches to identifying and capturing clinical errors resulting from AI deployed in healthcare settings as well as specifications for a central tracking repository for associated incidents that cause harm, including through bias or discrimination, to patients, caregivers, or other parties;

(B) analyzes captured data and generated evidence to develop, wherever appropriate, recommendations, best practices, or other informal guidelines aimed at avoiding these harms; and

(C) disseminates those recommendations, best practices, or other informal guidance to appropriate stakeholders, including healthcare providers.

(v) Within 365 days of the date of this order, the Secretary of HHS shall develop a strategy for regulating the use of AI or AI-enabled tools in drug-development processes. The strategy shall, at a minimum:

(A) define the objectives, goals, and high-level principles required for appropriate regulation throughout each phase of drug development;

(B) identify areas where future rulemaking, guidance, or additional statutory authority may be necessary to implement such a regulatory system;

(C) identify the existing budget, resources, personnel, and potential for new public/private partnerships necessary for such a regulatory system; and

(D) consider risks identified by the actions undertaken to implement section 4 of this order.

(c) To promote the safe and responsible development and use of AI in the transportation sector, in consultation with relevant agencies:

(i) Within 30 days of the date of this order, the Secretary of Transportation shall direct the Nontraditional and Emerging Transportation Technology (NETT) Council to assess the need for information, technical assistance, and guidance regarding the use of AI in transportation. The Secretary of Transportation shall further direct the NETT Council, as part of any such efforts, to:

(A) support existing and future initiatives to pilot transportation-related applications of AI, as they align with policy priorities articulated in the Department of Transportation's (DOT) Innovation Principles, including, as appropriate, through technical assistance and connecting stakeholders;

(B) evaluate the outcomes of such pilot programs in order to assess when DOT, or other Federal or State agencies, have sufficient information to take regulatory actions, as appropriate, and recommend appropriate actions when that information is available; and

(C) establish a new DOT Cross-Modal Executive Working Group, which will consist of members from different divisions of DOT and coordinate applicable work among these divisions, to solicit and use relevant input from appropriate stakeholders.

(ii) Within 90 days of the date of this order, the Secretary of Transportation shall direct appropriate Federal Advisory Committees of the DOT to provide advice on the safe and responsible use of AI in transportation. The committees shall include the Advanced Aviation Advisory Committee, the Transforming Transportation Advisory Committee, and the Intelligent Transportation Systems Program Advisory Committee.

(iii) Within 180 days of the date of this order, the Secretary of Transportation shall direct the Advanced Research Projects Agency-Infrastructure (ARPA-I) to explore the transportation-related opportunities and challenges of AI — including regarding software-defined AI enhancements impacting autonomous mobility ecosystems. The Secretary of Transportation shall further encourage ARPA-I to prioritize the allocation of grants to those opportunities, as appropriate. The work tasked to ARPA-I shall include soliciting input on these topics through a public consultation process, such as an RFI.

(d) To help ensure the responsible development and deployment of AI in the education sector, the Secretary of Education shall, within 365 days of the date of this order, develop resources, policies, and guidance regarding AI. These resources shall address safe, responsible, and nondiscriminatory uses of AI in education, including the impact AI systems have on vulnerable and underserved communities, and shall be developed in consultation with stakeholders as appropriate. They shall also include the development of an "AI toolkit" for education leaders implementing recommendations from the Department of Education's AI and the Future of Teaching and Learning report, including appropriate human review of AI decisions, designing AI systems to enhance trust and safety and align with privacy-related laws and regulations in the educational context, and developing education-specific guardrails.

(e) The Federal Communications Commission is encouraged to consider actions related to how AI will affect communications networks and consumers, including by:

(i) examining the potential for AI to improve spectrum management, increase the efficiency of non-Federal spectrum usage, and expand opportunities for the sharing of non-Federal spectrum;

(ii) coordinating with the National Telecommunications and Information Administration to create opportunities for sharing spectrum between Federal and non-Federal spectrum operations;

(iii) providing support for efforts to improve network security, resiliency, and interoperability using next-generation technologies that incorporate AI, including self-healing networks, 6G, and Open RAN; and

(iv) encouraging, including through rulemaking, efforts to combat unwanted robocalls and robotexts that are facilitated or exacerbated by AI and to deploy AI technologies that better serve consumers by blocking unwanted robocalls and robotexts.

Sec. 9. Protecting Privacy. (a) To mitigate privacy risks potentially exacerbated by AI — including by AI's facilitation of the collection or use of information about individuals, or the making of inferences about individuals — the Director of OMB shall:

(i) evaluate and take steps to identify commercially available information (CAI) procured by agencies, particularly CAI that contains personally identifiable information and including CAI procured from data brokers and CAI procured and processed indirectly through vendors, in appropriate agency inventory and reporting processes (other than when it is used for the purposes of national security);

(ii) evaluate, in consultation with the Federal Privacy Council and the Interagency Council on Statistical Policy, agency standards and procedures associated with the collection, processing, maintenance, use, sharing, dissemination, and disposition of CAI that contains personally identifiable information (other than when it is used for the purposes of national security) to inform potential guidance to agencies on ways to mitigate privacy and confidentiality risks from agencies' activities related to CAI;

(iii) within 180 days of the date of this order, in consultation with the Attorney General, the Assistant to the President for Economic Policy, and the

Director of OSTP, issue an RFI to inform potential revisions to guidance to agencies on implementing the privacy provisions of the E-Government Act of 2002 (Public Law 107-347). The RFI shall seek feedback regarding how privacy impact assessments may be more effective at mitigating privacy risks, including those that are further exacerbated by AI; and

(iv) take such steps as are necessary and appropriate, consistent with applicable law, to support and advance the near-term actions and long-term strategy identified through the RFI process, including issuing new or updated guidance or RFIs or consulting other agencies or the Federal Privacy Council.

(b) Within 365 days of the date of this order, to better enable agencies to use PETs to safeguard Americans' privacy from the potential threats exacerbated by AI, the Secretary of Commerce, acting through the Director of NIST, shall create guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI. The guidelines shall, at a minimum, describe the significant factors that bear on differential-privacy safeguards and common risks to realizing differential privacy in practice.

(c) To advance research, development, and implementation related to PETs:

(i) Within 120 days of the date of this order, the Director of NSF, in collaboration with the Secretary of Energy, shall fund the creation of a Research Coordination Network (RCN) dedicated to advancing privacy research and, in particular, the development, deployment, and scaling of PETs. The RCN shall serve to enable privacy researchers to share information, coordinate and collaborate in research, and develop standards for the privacy-research community.

(ii) Within 240 days of the date of this order, the Director of NSF shall engage with agencies to identify ongoing work and potential opportunities to incorporate PETs into their operations. The Director of NSF shall, where feasible and appropriate, prioritize research — including efforts to translate research discoveries into practical applications — that encourage the adoption of leading-edge PETs solutions for agencies' use, including through research engagement through the RCN described in subsection (c)(i) of this section.

(iii) The Director of NSF shall use the results of the United States-United Kingdom PETs Prize Challenge to inform the approaches taken, and opportunities identified, for PETs research and adoption.

Sec. 10. Advancing Federal Government Use of AI.

10.1. Providing Guidance for AI Management. (a) To coordinate the use of AI across the Federal Government, within 60 days of the date of this order and on an ongoing basis as necessary, the Director of OMB shall convene and chair an interagency council to coordinate the development and use of AI in agencies' programs and operations, other than the use of AI in national security systems. The Director of OSTP shall serve as Vice Chair for the interagency council. The interagency council's membership shall include, at minimum, the heads of the agencies identified in 31 U.S.C. 901(b), the Director of National Intelligence, and other agencies as identified by the Chair. Until agencies designate their permanent Chief AI Officers consistent with the guidance described in subsection 10.1(b) of this section, they shall be represented on the interagency council by an appropriate official at the Assistant Secretary level or equivalent, as determined by the head of each agency.

(b) To provide guidance on Federal Government use of AI, within 150 days of the date of this order and updated periodically thereafter, the Director of OMB, in coordination with the Director of OSTP, and in consultation with the interagency council established in subsection 10.1(a) of this section, shall issue guidance to agencies to strengthen the effective and appropriate use of AI, advance AI innovation, and manage risks from AI in the Federal Government. The Director of OMB's guidance shall specify, to the extent appropriate and consistent with applicable law:

(i) the requirement to designate at each agency within 60 days of the issuance of the guidance a Chief Artificial Intelligence Officer who shall hold primary responsibility in their agency, in coordination with other responsible officials, for coordinating their agency's use of AI, promoting AI innovation in their agency, managing risks from their agency's use of AI, and carrying out the responsibilities described in section 8(c) of Executive Order 13960 of

December 3, 2020 (Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government), and section 4(b) of Executive Order 14091;

(ii) the Chief Artificial Intelligence Officers' roles, responsibilities, seniority, position, and reporting structures;

(iii) for the agencies identified in 31 U.S.C. 901(b), the creation of internal Artificial Intelligence Governance Boards, or other appropriate mechanisms, at each agency within 60 days of the issuance of the guidance to coordinate and govern AI issues through relevant senior leaders from across the agency;

(iv) required minimum risk-management practices for Government uses of AI that impact people's rights or safety, including, where appropriate, the following practices derived from OSTP's Blueprint for an AI Bill of Rights and the NIST AI Risk Management Framework: conducting public consultation; assessing data quality; assessing and mitigating disparate impacts and algorithmic discrimination; providing notice of the use of AI; continuously monitoring and evaluating deployed AI; and granting human consideration and remedies for adverse decisions made using AI;

(v) specific Federal Government uses of AI that are presumed by default to impact rights or safety;

(vi) recommendations to agencies to reduce barriers to the responsible use of AI, including barriers related to information technology infrastructure, data, workforce, budgetary restrictions, and cybersecurity processes;

(vii) requirements that agencies identified in 31 U.S.C. 901(b) develop AI strategies and pursue high-impact AI use cases;

(viii) in consultation with the Secretary of Commerce, the Secretary of Homeland Security, and the heads of other appropriate agencies as determined by the Director of OMB, recommendations to agencies regarding:

(A) external testing for AI, including AI red-teaming for generative AI, to be developed in coordination with the Cybersecurity and Infrastructure Security Agency;

(B) testing and safeguards against discriminatory, misleading, inflammatory, unsafe, or deceptive outputs, as well as against producing child sexual abuse material and against producing non-consensual intimate imagery of real individuals (including intimate digital depictions of the body or body parts of an identifiable individual), for generative AI;

(C) reasonable steps to watermark or otherwise label output from generative AI;

(D) application of the mandatory minimum risk-management practices defined under subsection 10.1(b)(iv) of this section to procured AI;

(E) independent evaluation of vendors' claims concerning both the effectiveness and risk mitigation of their AI offerings;

(F) documentation and oversight of procured AI;

(G) maximizing the value to agencies when relying on contractors to use and enrich Federal Government data for the purposes of AI development and operation;

(H) provision of incentives for the continuous improvement of procured AI; and

(I) training on AI in accordance with the principles set out in this order and in other references related to AI listed herein; and

(ix) requirements for public reporting on compliance with this guidance.

(c) To track agencies' AI progress, within 60 days of the issuance of the guidance established in subsection 10.1(b) of this section and updated periodically thereafter, the Director of OMB shall develop a method for agencies to track and assess their ability to adopt AI into their programs and operations, manage its risks, and comply with Federal policy on AI. This method should draw on existing related efforts as appropriate and should address, as appropriate and consistent with applicable law, the practices, processes, and capabilities necessary for responsible AI adoption, training, and governance across, at a minimum, the areas of information technology infrastructure, data, workforce, leadership, and risk management.

(d) To assist agencies in implementing the guidance to be established in subsection 10.1(b) of this section:

(i) within 90 days of the issuance of the guidance, the Secretary of Commerce, acting through the Director of NIST, and in coordination with the Director of OMB and the Director of OSTP, shall develop guidelines, tools, and practices to support implementation of the minimum risk-management practices described in subsection 10.1(b)(iv) of this section; and

(ii) within 180 days of the issuance of the guidance, the Director of OMB shall develop an initial means to ensure that agency contracts for the acquisition of AI systems and services align with the guidance described in subsection 10.1(b) of this section and advance the other aims identified in section 7224(d)(1) of the Advancing American AI Act (Public Law 117-263, div. G, title LXXII, subtitle B).

(e) To improve transparency for agencies' use of AI, the Director of OMB shall, on an annual basis, issue instructions to agencies for the collection, reporting, and publication of agency AI use cases, pursuant to section 7225(a) of the Advancing American AI Act. Through these instructions, the Director shall, as appropriate, expand agencies' reporting on how they are managing risks from their AI use cases and update or replace the guidance originally established in section 5 of Executive Order 13960.

(f) To advance the responsible and secure use of generative AI in the Federal Government:

(i) As generative AI products become widely available and common in online platforms, agencies are discouraged from imposing broad general bans or blocks on agency use of generative AI. Agencies should instead limit access, as necessary, to specific generative AI services based on specific risk assessments; establish guidelines and limitations on the appropriate use of generative AI; and, with appropriate safeguards in place, provide their personnel and programs with access to secure and reliable generative AI capabilities, at least for the purposes of experimentation and routine tasks that carry a low risk of impacting Americans' rights. To protect Federal Government information, agencies are also encouraged to employ risk-management practices, such as training their staff on proper use, protection, dissemination, and disposition of Federal information; negotiating appropriate terms of service with vendors; implementing measures designed to ensure compliance with record-keeping, cybersecurity, confidentiality, privacy, and data protection requirements; and deploying other measures to prevent misuse of Federal Government information in generative AI.

(ii) Within 90 days of the date of this order, the Administrator of General Services, in coordination with the Director of OMB, and in consultation with the Federal Secure Cloud Advisory Committee and other relevant agencies as the Administrator of General Services may deem appropriate, shall develop and issue a framework for prioritizing critical and emerging technologies offerings in the Federal Risk and Authorization Management Program authorization process, starting with generative AI offerings that have the primary purpose of providing large language model-based chat interfaces, code-generation and debugging tools, and associated application programming interfaces, as well as prompt-based image generators. This framework shall apply for no less than 2 years from the date of its issuance. Agency Chief Information Officers, Chief Information Security Officers, and authorizing officials are also encouraged to prioritize generative AI and other critical and emerging technologies in granting authorities for agency operation of information technology systems and any other applicable release or oversight processes, using continuous authorizations and approvals wherever feasible.

(iii) Within 180 days of the date of this order, the Director of the Office of Personnel Management (OPM), in coordination with the Director of OMB, shall develop guidance on the use of generative AI for work by the Federal workforce.

(g) Within 30 days of the date of this order, to increase agency investment in AI, the Technology Modernization Board shall consider, as it deems appropriate and consistent with applicable law, prioritizing funding for AI projects for the Technology Modernization Fund for a period of at least 1 year. Agencies are encouraged to submit to the Technology Modernization Fund project funding proposals that include AI — and particularly generative AI — in service of mission delivery.

(h) Within 180 days of the date of this order, to facilitate agencies' access to commercial AI capabilities, the Administrator of General Services, in coordination with the Director of OMB, and in collaboration with the

Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, the Administrator of the National Aeronautics and Space Administration, and the head of any other agency identified by the Administrator of General Services, shall take steps consistent with applicable law to facilitate access to Federal Government-wide acquisition solutions for specified types of AI services and products, such as through the creation of a resource guide or other tools to assist the acquisition workforce. Specified types of AI capabilities shall include generative AI and specialized computing infrastructure.

(i) The initial means, instructions, and guidance issued pursuant to subsections 10.1(a)-(h) of this section shall not apply to AI when it is used as a component of a national security system, which shall be addressed by the proposed National Security Memorandum described in subsection 4.8 of this order.

10.2. Increasing AI Talent in Government. (a) Within 45 days of the date of this order, to plan a national surge in AI talent in the Federal Government, the Director of OSTP and the Director of OMB, in consultation with the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy, the Assistant to the President and Domestic Policy Advisor, and the Assistant to the President and Director of the Gender Policy Council, shall identify priority mission areas for increased Federal Government AI talent, the types of talent that are highest priority to recruit and develop to ensure adequate implementation of this order and use of relevant enforcement and regulatory authorities to address AI risks, and accelerated hiring pathways.

(b) Within 45 days of the date of this order, to coordinate rapid advances in the capacity of the Federal AI workforce, the Assistant to the President and Deputy Chief of Staff for Policy, in coordination with the Director of OSTP and the Director of OMB, and in consultation with the National Cyber Director, shall convene an AI and Technology Talent Task Force, which shall include the Director of OPM, the Director of the General Services Administration's Technology Transformation Services, a representative from the Chief Human Capital Officers Council, the Assistant to the President for Presidential Personnel, members of appropriate agency technology talent programs, a representative of the Chief Data Officer Council, and a representative of the interagency council convened under subsection 10.1(a) of this section. The Task Force's purpose shall be to accelerate and track the hiring of AI and AI-enabling talent across the Federal Government, including through the following actions:

(i) within 180 days of the date of this order, tracking and reporting progress to the President on increasing AI capacity across the Federal Government, including submitting to the President a report and recommendations for further increasing capacity;

(ii) identifying and circulating best practices for agencies to attract, hire, retain, train, and empower AI talent, including diversity, inclusion, and accessibility best practices, as well as to plan and budget adequately for AI workforce needs;

(iii) coordinating, in consultation with the Director of OPM, the use of fellowship programs and agency technology-talent programs and human-capital teams to build hiring capabilities, execute hires, and place AI talent to fill staffing gaps; and

(iv) convening a cross-agency forum for ongoing collaboration between AI professionals to share best practices and improve retention.

(c) Within 45 days of the date of this order, to advance existing Federal technology talent programs, the United States Digital Service, Presidential Innovation Fellowship, United States Digital Corps, OPM, and technology talent programs at agencies, with support from the AI and Technology Talent Task Force described in subsection 10.2(b) of this section, as appropriate and permitted by law, shall develop and begin to implement plans to support the rapid recruitment of individuals as part of a Federal Government-wide AI talent surge to accelerate the placement of key AI and AI-enabling talent in high-priority areas and to advance agencies' data and technology strategies.

(d) To meet the critical hiring need for qualified personnel to execute the initiatives in this order, and to improve Federal hiring practices for AI talent, the Director of OPM, in consultation with the Director of OMB, shall:

(i) within 60 days of the date of this order, conduct an evidence-based review on the need for hiring and workplace flexibility, including Federal Government-wide direct-hire authority for AI and related data-science and technical roles, and, where the Director of OPM finds such authority is appropriate, grant it; this review shall include the following job series at all General Schedule (GS) levels: IT Specialist (2210), Computer Scientist (1550), Computer Engineer (0854), and Program Analyst (0343) focused on AI, and any subsequently developed job series derived from these job series;

(ii) within 60 days of the date of this order, consider authorizing the use of excepted service appointments under 5 C.F.R. 213.3102(i)(3) to address the need for hiring additional staff to implement directives of this order;

(iii) within 90 days of the date of this order, coordinate a pooled-hiring action informed by subject-matter experts and using skills-based assessments to support the recruitment of AI talent across agencies;

(iv) within 120 days of the date of this order, as appropriate and permitted by law, issue guidance for agency application of existing pay flexibilities or incentive pay programs for AI, AI-enabling, and other key technical positions to facilitate appropriate use of current pay incentives;

(v) within 180 days of the date of this order, establish guidance and policy on skills-based, Federal Government-wide hiring of AI, data, and technology talent in order to increase access to those with nontraditional academic backgrounds to Federal AI, data, and technology roles;

(vi) within 180 days of the date of this order, establish an interagency working group, staffed with both human-resources professionals and recruiting technical experts, to facilitate Federal Government-wide hiring of people with AI and other technical skills;

(vii) within 180 days of the date of this order, review existing Executive Core Qualifications (ECQs) for Senior Executive Service (SES) positions informed by data and AI literacy competencies and, within 365 days of the date of this order, implement new ECQs as appropriate in the SES assessment process;

(viii) within 180 days of the date of this order, complete a review of competencies for civil engineers (GS-0810 series) and, if applicable, other related occupations, and make recommendations for ensuring that adequate

AI expertise and credentials in these occupations in the Federal Government reflect the increased use of AI in critical infrastructure; and

(ix) work with the Security, Suitability, and Credentialing Performance Accountability Council to assess mechanisms to streamline and accelerate personnel-vetting requirements, as appropriate, to support AI and fields related to other critical and emerging technologies.

(e) To expand the use of special authorities for AI hiring and retention, agencies shall use all appropriate hiring authorities, including Schedule A(r) excepted service hiring and direct-hire authority, as applicable and appropriate, to hire AI talent and AI-enabling talent rapidly. In addition to participating in OPM-led pooled hiring actions, agencies shall collaborate, where appropriate, on agency-led pooled hiring under the Competitive Service Act of 2015 (Public Law 114-137) and other shared hiring. Agencies shall also, where applicable, use existing incentives, pay-setting authorities, and other compensation flexibilities, similar to those used for cyber and information technology positions, for AI and data-science professionals, as well as plain-language job titles, to help recruit and retain these highly skilled professionals. Agencies shall ensure that AI and other related talent needs (such as technology governance and privacy) are reflected in strategic workforce planning and budget formulation.

(f) To facilitate the hiring of data scientists, the Chief Data Officer Council shall develop a position-description library for data scientists (job series 1560) and a hiring guide to support agencies in hiring data scientists.

(g) To help train the Federal workforce on AI issues, the head of each agency shall implement — or increase the availability and use of — AI training and familiarization programs for employees, managers, and leadership in technology as well as relevant policy, managerial, procurement, regulatory, ethical, governance, and legal fields. Such training programs should, for example, empower Federal employees, managers, and leaders to develop and maintain an operating knowledge of emerging AI technologies to assess opportunities to use these technologies to enhance the delivery of services to the public, and to mitigate risks associated with these technologies. Agencies that provide professional-development opportunities, grants, or funds for their staff should take appropriate steps to ensure that employees who do not serve in traditional technical roles, such as policy, managerial, procurement, or legal fields, are nonetheless eligible to receive funding for programs and courses that focus on AI, machine learning, data science, or other related subject areas.

(h) Within 180 days of the date of this order, to address gaps in AI talent for national defense, the Secretary of Defense shall submit a report to the President through the Assistant to the President for National Security Affairs that includes:

(i) recommendations to address challenges in the Department of Defense's ability to hire certain noncitizens, including at the Science and Technology Reinvention Laboratories;

(ii) recommendations to clarify and streamline processes for accessing classified information for certain noncitizens through Limited Access Authorization at Department of Defense laboratories;

(iii) recommendations for the appropriate use of enlistment authority under 10 U.S.C. 504(b)(2) for experts in AI and other critical and emerging technologies; and

(iv) recommendations for the Department of Defense and the Department of Homeland Security to work together to enhance the use of appropriate authorities for the retention of certain noncitizens of vital importance to national security by the Department of Defense and the Department of Homeland Security.

Sec. 11. Strengthening American Leadership Abroad. (a) To strengthen United States leadership of global efforts to unlock AI's potential and meet its challenges, the Secretary of State, in coordination with the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy, the Director of OSTP, and the heads of other relevant agencies as appropriate, shall:

(i) lead efforts outside of military and intelligence areas to expand engagements with international allies and partners in relevant bilateral, multilateral, and multi-stakeholder fora to advance those allies' and partners' understanding of existing and planned AI-related guidance and policies of the United States, as well as to enhance international collaboration; and

(ii) lead efforts to establish a strong international framework for managing the risks and harnessing the benefits of AI, including by encouraging international allies and partners to support voluntary commitments similar to those that United States companies have made in pursuit of these objectives and coordinating the activities directed by subsections (b), (c), (d), and (e) of this section, and to develop common regulatory and other accountability principles for foreign nations, including to manage the risk that AI systems pose.

(b) To advance responsible global technical standards for AI development and use outside of military and intelligence areas, the Secretary of Commerce, in coordination with the Secretary of State and the heads of other relevant agencies as appropriate, shall lead preparations for a coordinated effort with key international allies and partners and with standards development organizations, to drive the development and implementation of AI-related consensus standards, cooperation and coordination, and information sharing. In particular, the Secretary of Commerce shall:

(i) within 270 days of the date of this order, establish a plan for global engagement on promoting and developing AI standards, with lines of effort that may include:

(A) AI nomenclature and terminology;

(B) best practices regarding data capture, processing, protection, privacy, confidentiality, handling, and analysis;

(C) trustworthiness, verification, and assurance of AI systems; and

(D) AI risk management;

(ii) within 180 days of the date the plan is established, submit a report to the President on priority actions taken pursuant to the plan; and

(iii) ensure that such efforts are guided by principles set out in the NIST AI Risk Management Framework and United States Government National Standards Strategy for Critical and Emerging Technology.

(c) Within 365 days of the date of this order, to promote safe, responsible, and rights-affirming development and deployment of AI abroad:

(i) The Secretary of State and the Administrator of the United States Agency for International Development, in coordination with the Secretary of Commerce, acting through the director of NIST, shall publish an AI in Global Development Playbook that incorporates the AI Risk Management Framework's principles, guidelines, and best practices into the social, technical, economic, governance, human rights, and security conditions of contexts beyond United States borders. As part of this work, the Secretary of State and the Administrator of the United States Agency for International Development shall draw on lessons learned from programmatic uses of AI in global development.

(ii) The Secretary of State and the Administrator of the United States Agency for International Development, in collaboration with the Secretary of Energy and the Director of NSF, shall develop a Global AI Research Agenda to guide the objectives and implementation of AI-related research in contexts beyond United States borders. The Agenda shall:

(A) include principles, guidelines, priorities, and best practices aimed at ensuring the safe, responsible, beneficial, and sustainable global development and adoption of AI; and

(B) address AI's labor-market implications across international contexts, including by recommending risk mitigations.

(d) To address cross-border and global AI risks to critical infrastructure, the Secretary of Homeland Security, in coordination with the Secretary of State, and in consultation with the heads of other relevant agencies as the Secretary of Homeland Security deems appropriate, shall lead efforts with international allies and partners to enhance cooperation to prevent, respond to, and recover from potential critical infrastructure disruptions resulting from incorporation of AI into critical infrastructure systems or malicious use of AI.

(i) Within 270 days of the date of this order, the Secretary of Homeland Security, in coordination with the Secretary of State, shall develop a plan for multilateral engagements to encourage the adoption of the AI safety and security guidelines for use by critical infrastructure owners and operators developed in section 4.3(a) of this order.

(ii) Within 180 days of establishing the plan described in subsection (d)(i) of this section, the Secretary of Homeland Security shall submit a report to the President on priority actions to mitigate cross-border risks to critical United States infrastructure.

Sec. 12. Implementation. (a) There is established, within the Executive Office of the President, the White House Artificial Intelligence Council (White House AI Council). The function of the White House AI Council is to coordinate the activities of agencies across the Federal Government to ensure the effective formulation, development, communication, industry engagement related to, and timely implementation of AI-related policies, including policies set forth in this order.

(b) The Assistant to the President and Deputy Chief of Staff for Policy shall serve as Chair of the White House AI Council.

(c) In addition to the Chair, the White House AI Council shall consist of the following members, or their designees:

(i) the Secretary of State;

(ii) the Secretary of the Treasury;

(iii) the Secretary of Defense;

(iv) the Attorney General;

(v) the Secretary of Agriculture;

(vi) the Secretary of Commerce;

(vii) the Secretary of Labor;

(viii) the Secretary of HHS;

(ix) the Secretary of Housing and Urban Development;

(x) the Secretary of Transportation;

(xi) the Secretary of Energy;

(xii) the Secretary of Education;

(xiii) the Secretary of Veterans Affairs;

(xiv) the Secretary of Homeland Security;

(xv) the Administrator of the Small Business Administration;

(xvi) the Administrator of the United States Agency for International Development;

(xvii) the Director of National Intelligence;

(xviii) the Director of NSF;

(xix) the Director of OMB;

(xx) the Director of OSTP;

(xxi) the Assistant to the President for National Security Affairs;

(xxii) the Assistant to the President for Economic Policy;

(xxiii) the Assistant to the President and Domestic Policy Advisor;

(xxiv) the Assistant to the President and Chief of Staff to the Vice President;

(xxv) the Assistant to the President and Director of the Gender Policy Council;

(xxvi) the Chairman of the Council of Economic Advisers;

(xxvii) the National Cyber Director;

(xxviii) the Chairman of the Joint Chiefs of Staff; and

(xxix) the heads of such other agencies, independent regulatory agencies, and executive offices as the Chair may from time to time designate or invite to participate.

(d) The Chair may create and coordinate subgroups consisting of White House AI Council members or their designees, as appropriate.

Sec. 13. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

THE WHITE HOUSE,
October 30, 2023.

OCTOBER 30, 2023

FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

Today, President Biden is issuing a landmark Executive Order to ensure that America leads the way in seizing the promise and managing the risks of artificial intelligence (AI). The Executive Order establishes new standards for AI safety and security, protects Americans' privacy, advances equity and civil rights, stands up for consumers and workers, promotes innovation and competition, advances American leadership around the world, and more.

As part of the Biden-Harris Administration's comprehensive strategy for responsible innovation, the Executive Order builds on previous actions the President has taken, including work that led to voluntary commitments from 15 leading companies to drive safe, secure, and trustworthy development of AI.

The Executive Order directs the following actions:

New Standards for AI Safety and Security

As AI's capabilities grow, so do its implications for Americans' safety and security. **With this Executive Order, the President directs the most sweeping actions ever taken to protect Americans from the potential risks of AI systems:**

- **Require that developers of the most powerful AI systems share their safety test results and other critical information with the U.S. government.** In accordance with the Defense Production Act, the Order will require that companies developing any foundation model that poses a serious risk to national security, national economic security, or national public health and safety must notify the federal government when training the model, and must share the results of all red-team safety tests. These measures will ensure AI systems are safe, secure, and trustworthy before companies make them public.

- **Develop standards, tools, and tests to help ensure that AI systems are safe, secure, and trustworthy.** The National Institute of Standards and Technology will set the rigorous standards for extensive red-team testing to ensure safety before public release. The Department of Homeland Security will apply those standards to critical infrastructure sectors and establish the AI Safety and Security Board. The Departments of Energy and Homeland Security will also address AI systems' threats to critical infrastructure, as well as chemical, biological, radiological, nuclear, and cybersecurity risks. Together, these are the most significant actions ever taken by any government to advance the field of AI safety.

- **Protect against the risks of using AI to engineer dangerous biological materials** by developing strong new standards for biological synthesis screening. Agencies that fund life-science projects will establish these standards as a condition of federal funding, creating powerful incentives to ensure appropriate screening and manage risks potentially made worse by AI.

- **Protect Americans from AI-enabled fraud and deception by establishing standards and best practices for detecting AI-generated content and authenticating official content**. The Department of Commerce will develop guidance for content authentication and watermarking to clearly label AI-generated content. Federal agencies will use these tools to make it easy for Americans to know that the communications they receive from their government are authentic—and set an example for the private sector and governments around the world.

- **Establish an advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software,** building on the Biden-Harris Administration's ongoing AI Cyber Challenge. Together, these efforts will harness AI's potentially game-changing cyber capabilities to make software and networks more secure.

- **Order the development of a National Security Memorandum that directs further actions on AI and security,** to be developed by the National Security Council and White House Chief of Staff. This document will ensure that the United States military and intelligence community use AI safely, ethically, and effectively in their missions, and will direct actions to counter adversaries' military use of AI.

Protecting Americans' Privacy

Without safeguards, AI can put Americans' privacy further at risk. AI not only makes it easier to extract, identify, and exploit personal data, but it also heightens incentives to do so because companies use data to train AI systems. **To better protect Americans' privacy, including from the risks posed by AI, the President calls on Congress to pass bipartisan data privacy legislation to protect all Americans, especially kids, and directs the following actions:**

- **Protect Americans' privacy by prioritizing federal support for accelerating the development and use of privacy-preserving techniques—**including ones that use cutting-edge AI and that let AI systems be trained while preserving the privacy of the training data.
- **Strengthen privacy-preserving research and technologies,** such as cryptographic tools that preserve individuals' privacy, by funding a Research Coordination Network to advance rapid breakthroughs and development. The National Science Foundation will also work with this network to promote the adoption of leading-edge privacy-preserving technologies by federal agencies.
- **Evaluate how agencies collect and use commercially available information**—including information they procure from data brokers—and **strengthen privacy guidance for federal agencies** to account for AI risks. This work will focus in particular on commercially available information containing personally identifiable data.
- **Develop guidelines for federal agencies to evaluate the effectiveness of privacy-preserving techniques,** including those used in AI systems. These guidelines will advance agency efforts to protect Americans' data.

Advancing Equity and Civil Rights

Irresponsible uses of AI can lead to and deepen discrimination, bias, and other abuses in justice, healthcare, and housing. The Biden-Harris Administration has already taken action by publishing the Blueprint for an AI

Bill of Rights and issuing an Executive Order directing agencies to combat algorithmic discrimination, while enforcing existing authorities to protect people's rights and safety. **To ensure that AI advances equity and civil rights, the President directs the following additional actions:**

- **Provide clear guidance to landlords, Federal benefits programs, and federal contractors** to keep AI algorithms from being used to exacerbate discrimination.
- **Address algorithmic discrimination** through training, technical assistance, and coordination between the Department of Justice and Federal civil rights offices on best practices for investigating and prosecuting civil rights violations related to AI.
- **Ensure fairness throughout the criminal justice system** by developing best practices on the use of AI in sentencing, parole and probation, pretrial release and detention, risk assessments, surveillance, crime forecasting and predictive policing, and forensic analysis.

Standing Up for Consumers, Patients, and Students

AI can bring real benefits to consumers—for example, by making products better, cheaper, and more widely available. But AI also raises the risk of injuring, misleading, or otherwise harming Americans. **To protect consumers while ensuring that AI can make Americans better off, the President directs the following actions:**

- **Advance the responsible use of AI** in healthcare and the development of affordable and life-saving drugs. The Department of Health and Human Services will also establish a safety program to receive reports of —and act to remedy – harms or unsafe healthcare practices involving AI.
- **Shape AI's potential to transform education** by creating resources to support educators deploying AI-enabled educational tools, such as personalized tutoring in schools.

Supporting Workers

AI is changing America's jobs and workplaces, offering both the promise of improved productivity but also the dangers of increased workplace surveillance, bias, and job displacement. **To mitigate these risks, support**

workers' ability to bargain collectively, and invest in workforce training and development that is accessible to all, the President directs the following actions:

- **Develop principles and best practices to mitigate the harms and maximize the benefits of AI for workers** by addressing job displacement; labor standards; workplace equity, health, and safety; and data collection. These principles and best practices will benefit workers by providing guidance to prevent employers from undercompensating workers, evaluating job applications unfairly, or impinging on workers' ability to organize.
- **Produce a report on AI's potential labor-market impacts**, and **study and identify options for strengthening federal support for workers facing labor disruptions**, including from AI.

Promoting Innovation and Competition

America already leads in AI innovation—more AI startups raised first-time capital in the United States last year than in the next seven countries combined. **The Executive Order ensures that we continue to lead the way in innovation and competition through the following actions:**

- **Catalyze AI research across the United States** through a pilot of the National AI Research Resource—a tool that will provide AI researchers and students access to key AI resources and data—and expanded grants for AI research in vital areas like healthcare and climate change.
- **Promote a fair, open, and competitive AI ecosystem** by providing small developers and entrepreneurs access to technical assistance and resources, helping small businesses commercialize AI breakthroughs, and encouraging the Federal Trade Commission to exercise its authorities.
- **Use existing authorities to expand the ability of highly skilled immigrants and nonimmigrants with expertise in critical areas to study, stay, and work in the United States** by modernizing and streamlining visa criteria, interviews, and reviews.

Advancing American Leadership Abroad

AI's challenges and opportunities are global. **The Biden-Harris Administration will continue working with other nations to support safe, secure, and trustworthy deployment and use of AI worldwide. To that end, the President directs the following actions:**

- **Expand bilateral, multilateral, and multistakeholder engagements to collaborate on AI**. The State Department, in collaboration, with the Commerce Department will lead an effort to establish robust international frameworks for harnessing AI's benefits and managing its risks and ensuring safety. In addition, this week, Vice President Harris will speak at the UK Summit on AI Safety, hosted by Prime Minister Rishi Sunak.
- **Accelerate development and implementation of vital AI standards** with international partners and in standards organizations, ensuring that the technology is safe, secure, trustworthy, and interoperable.
- **Promote the safe, responsible, and rights-affirming development and deployment of AI abroad to solve global challenges,** such as advancing sustainable development and mitigating dangers to critical infrastructure.

Ensuring Responsible and Effective Government Use of AI

AI can help government deliver better results for the American people. It can expand agencies' capacity to regulate, govern, and disburse benefits, and it can cut costs and enhance the security of government systems. However, use of AI can pose risks, such as discrimination and unsafe decisions. **To ensure the responsible government deployment of AI and modernize federal AI infrastructure, the President directs the following actions:**

- **Issue guidance for agencies' use of AI,** including clear standards to protect rights and safety, improve AI procurement, and strengthen AI deployment.
- **Help agencies acquire specified AI products and services** faster, more cheaply, and more effectively through more rapid and efficient contracting.

- **Accelerate the rapid hiring of AI professionals** as part of a government-wide AI talent surge led by the Office of Personnel Management, U.S. Digital Service, U.S. Digital Corps, and Presidential Innovation Fellowship. Agencies will provide AI training for employees at all levels in relevant fields.

As we advance this agenda at home, the Administration will work with allies and partners abroad on a strong international framework to govern the development and use of AI. The Administration has already consulted widely on AI governance frameworks over the past several months—engaging with Australia, Brazil, Canada, Chile, the European Union, France, Germany, India, Israel, Italy, Japan, Kenya, Mexico, the Netherlands, New Zealand, Nigeria, the Philippines, Singapore, South Korea, the UAE, and the UK. The actions taken today support and complement Japan's leadership of the G-7 Hiroshima Process, the UK Summit on AI Safety, India's leadership as Chair of the Global Partnership on AI, and ongoing discussions at the United Nations.

The actions that President Biden directed today are vital steps forward in the U.S.'s approach on safe, secure, and trustworthy AI. More action will be required, and the Administration will continue to work with Congress to pursue bipartisan legislation to help America lead the way in responsible innovation.

For more on the Biden-Harris Administration's work to advance AI, and for opportunities to join the Federal AI workforce, visit AI.gov.

###

Lee D. Winston
lwinston@winstoncooks.com
Roderick T. Cooks
rcooks@winstoncooks.com
Winston Cooks, LLC
420 20th Street North
Suite#2200
Birmingham, AL 35203
Telephone: (205) 482-5174
Facsimile: (205) 278-5876

Attorneys for the Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DEREK L. MOBLEY, for and on behalf of himself and other persons similarly situated, Plaintiffs, vs. WORKDAY, INC. , Defendant.	)	**CLASS ACTION** **FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

NATURE OF COMPLAINT

Plaintiff, Derek L. Mobley ("Mobley" or "Representative Plaintiff") brings this suit for injunctive, monetary, and declarative relief against Defendant Workday, Inc. ("Workday") for engaging in a pattern or practice of illegal discrimination on the basis of race, age, and/or disability in violation of Title VII of the Civil Rights Act of 1964, the Civil Rights Act of 1866 ("42 U.S.C. § 1981), the Age Discrimination in Employment Act of 1967, and the ADA Amendments Act of 2008 ("ADAAA"). Defendant Workday, Inc.'s ("Workday" or "Defendant") continuous and systemic pattern or practice of discriminatory job screening-which disproportionately disqualifies African-Americans, individuals over the age of forty (40) and individuals with disabilities from securing gainful employment.

Workday provides human resource management services to medium-sized and large, global organizations that span numerous industry categories, including professional and business services, financial services, healthcare, education, government, technology, media, retail, and hospitality. Firms purchase a subscription to Workday's services and as part of their subscription, customers are provided applicant screening services to include professional consulting to enable them to use Workday applications. In May of 2023, the Bureau of Labor Statistics reported more than 9.8 million job openings in the U.S. Workday recruiting processed 2.2 million U.S. job requisition transactions in May, representing nearly 22% of all U.S. job openings that month. At that rate, Workday was projected to process more than 36 million requisitions, screen 266 million applications, and make 24 million job offers in 2023 alone. Workday processes this massive number of applications by using automated screening tools that rely on artificial intelligence.

Defendant Workday, Inc.'s artificial intelligence ("AI") systems and screening tools rely on algorithms and inputs created by humans who often have built-in motivations, conscious and unconscious, to discriminate. This discrimination is the result of a specific policy: Workday's decision to employ an automated system—in lieu of human judgment—to determine how the high-volume of applications it reviews should be processed for its clients-customers. Specifically, Workday uses machine-learning algorithms and artificial-intelligence tools (collectively "algorithmic decision-making tools") to screen out applicants who are African-American, disabled, and/or over the age of 40. Defendant Workday's algorithmic decisionmaking tools and applicant screening system determine whether an employer should accept or reject an application for employment based on the individual's race, age, and or disability.

All applicants who attempt to access employment via Workday's platform have been uniformly subject to this policy during the Class Period, including the Plaintiff and the proposed Class. It is thus reasonable to attribute any systematic difference in the rate of successful applicants to Workday's policy of using algorithmic decision-making tools to screen all applications. This causal connection is unsurprising: algorithmic decision-making tools have been known to cause bias in hiring.

Workday's automated system—for a variety of reasons that Workday should know about and could easily prevent—is much more likely to deny applicants who are African-American, suffer from disabilities and/or are over the age of 40. Because their applications are more likely to be flagged for rejection, African-American, disabled and over 40 applicants are disproportionately more likely to denied jobs. As a result, African-American, disabled, and those over 40, experience greater rates of rejection for employment which negatively impacts their career prospects, earnings, and quality of life.

The Plaintiff and, upon information and belief, the classes he seeks to represent have made numerous applications for employment using the Workday platform only to be rejected. Because of this high rate of rejection, Plaintiff, and the classes he seeks to represent have also been discouraged from seeking employment with firms that use the Workday hiring platform as such application is futile because of Workday's discriminatory algorithmic decision-making tools. The hiring discrimination African-Americans, the disabled, and those over the age of 40 have experienced and are experiencing because of Workday's discriminatory algorithmic decision-making tools cause tangible financial harm, and are unreasonable, vexatious, and humiliating. Accordingly, Plaintiffs seek damages as well as declaratory and injunctive relief.

JURISDICTION AND VENUE

1. The jurisdiction of this Court is invoked pursuant to 28 U.S.C. §§ 1331, 1343(3), and (4), 2201 and 2202, 42 U.S.C. 2000d-2 and 2000e5(f), and 29 U.S.C. § 621, et seq. Supplemental jurisdiction for the state law claims is invoked pursuant to 28 U.S.C. §1367.

2. This is a suit authorized and instituted pursuant to the Act of Congress known as Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000 et seq., as amended, "The Civil Rights Act of 1866," 42 U.S.C. § 1981, the Age Discrimination in Employment Act of 1967, 29 U.S.C. § 621, et seq., and the ADA Amendments Act of 2008 ("ADAAA").

3. Venue is proper in the Northern District of California under 28 U.S.C. § 1391(B) & (c) because Workday is located here and the acts complained of occurred in the Northern District of California.

PARTIES

4. Plaintiff, Derek Mobley is an African -American male, over the age of forty (40) and who suffers from depression and anxiety. Mr. Mobley is an applicant.

5. Defendant Workday is an employment agency pursuant to Section 703(b) of the Act, 42 U.S.C. § 2000e-2(b). Defendant Workday is also an agent of employers who have delegated to it authority to make decisions in the hiring process, including by relying on the results of selection procedures that Workday administers on the employers' behalf to make hiring decisions, alternatively Workday is an indirect employer because it controls access to employment opportunities. Defendant Workday's headquarters and principal place of business is located at 6110 Stoneridge Mall Road, Pleasanton, California.

CONDITIONS PRECEDENT TO SUIT UNDER TITLE VII, THE ADEA AND THE ADAAA

6. On June 3, 2021, Mr. Mobley filed a charge of discrimination with the Oakland Field Office of the United States Equal Employment Opportunity Commission. On July 19, 2021, Mr. Mobley filed an amended charge of discrimination. On November 22, 2022, the EEOC issued Mr. Mobley a Dismissal and Notice of Right to Sue, giving him ninety-days from its receipt to file a case. Thus, Mr. Mobley has satisfied all prerequisites to bring this action pursuant to Title VII, the ADEA, and the ADAAA.

7. Mr. Mobley's claims arising under 42 U.S.C. § 1981 do not require administrative exhaustion and are subject to a four-year statute of limitations. 28 U.S.C. § 1658.

CLASS ACTION ALLEGATIONS

8. The Representative Plaintiff brings this action in his own behalf and on behalf of all others similarly situated, pursuant to Rule 23 of the Federal Rules of Civil Procedure, and seek to represent the following subclasses:

•All African-American applicants or former applicants who from June 3, 2019, to the present were subjected to the challenged discriminatory screening process.

•All applicants or former applicants over the age of forty (40) who from June 3, 2019, to the present were subjected to the challenged discriminatory screening process.

•All applicants or former applicants who have a diagnosed mental health or cognitive condition who from June 3, 2019, to the present were required to take a Workday branded cognitive assessment or personality tests as part of the application process.

Mr. Mobley in the case at bar challenges systemic discrimination by, and seeks class-wide relief against, Workday for its utilization of discriminatory screening tools as part of its employment policies and procedures which constitute a pattern and practice of discrimination on the basis of race, age, and disability with respect to selections. These screening tools have been continuously utilized by the Defendant since at least 2017, and their implementation and use has personally harmed the named the Plaintiff, and the putative class members he seeks to represent. Workday's client-customers delegate to it the hiring process, recruitment, and onboarding of employees. Workday then utilizes screening tools, to include Workday branded assessments and/or tests, to s process and interpret an applicant's qualifications and recommend whether the applicant should be accepted or rejected.

Workday's utilization of these screening tools relies upon subjective practices which have caused disparate impact and disparate treatment to applicants who are African-American, over the age of forty (40) or and/or disabled. Applicants who are not members of these protected groups and who are similarly situated to the Representative Plaintiff, have not been subjected to such discriminatory treatment.

A. COMMON QUESTIONS OF LAW AND FACT

9. The prosecution of the claims of the Representative Plaintiff requires adjudication of numerous questions of law and fact common to his individual claims and those of the putative classes he seeks to represent. The common questions of law would include, inter alia: (a) whether the Defendant's screening products cause African-American, individuals over the age of forty (40), and/or individuals with a disability to be disproportionately and more likely denied employment; (b) whether the Defendant's doing so cannot be justified as a necessary business practice for evaluating potential employees; and (c) whether the Defendant's screening products have a disparate impact on applicants who are African-American, over the age of forty (40), and/or disabled in violation of the "Civil Rights Act of 1964," 42 U.S.C. § 2000 et seq., the "Civil Rights Act of 1866," 42 U.S.C. § 1981and 1981a, the Age Discrimination in Employment

Act of 1967, 29 U.S.C. § 621, et seq., and the ADA Amendments Act of 2008 ("ADAAA"). The common questions of fact would include, inter alia: (1) whether Workday's administration of its screening products discriminated against the aforementioned applicants because of their race, age, and/or disability with regards to hiring; (2) whether compensatory and punitive damages, injunctive relief, and other equitable remedies for the class are warranted; and (3) whether Workday discriminated against the aforementioned protected groups in other terms and conditions of employment. The details of the Representative Plaintiff's claims are encompassed within the claims prosecuted on behalf of the class and set forth in this Complaint.

B. TYPICALITY

10. The claims of the Representative Plaintiff are typical of those of the members of the class. The Representative Plaintiff and all class members have been and are similarly adversely affected by the systemic racially discriminatory practices complained of herein. Specifically, the representative claims, like those of the class members, arise out of Defendant's pervasive discriminatory conduct with regard to aforementioned discrimination in hiring and other terms and conditions of employment. The relief necessary to remedy the claims of the Representative Plaintiff is the same relief that is necessary to remedy the claims of the putative class members in this case. The Representative Plaintiff seeks the following relief for individual claims and class claims asserted herein: (1) declaratory judgment that Defendant has engaged in systemic discrimination against African-Americans, individuals over the age of forty (40), and/or the disabled; (2) a permanent injunction against such continuing discrimination; (3) injunctive relief which reforms Workday's screening products, policies, practices and procedures so that the Representative Plaintiff and the class members will be able to compete fairly in the future for jobs and enjoy terms and conditions of employment traditionally afforded similarly

situated employees outside of the protected categories; (4) backpay, front pay, compensatory damages, and other equitable remedies necessary to make the Plaintiff, and the class, whole from Workday's past discrimination; and, (5) attorneys' fees, costs, and expenses.

C. NUMEROSITY AND IMPRACTICABILITY OF JOINDER

11. The class that the Representative Plaintiff seeks to represent is too numerous to make joinder practicable. The proposed class consists of numerous former, current, and future applicants who have been denied employment due to the discriminatory administration of Workday's screening products. Workday's pattern or practice of discrimination also makes joinder impracticable by making it impractical and inefficient to identify many members of the class prior to the determination of the merits of Workday's class wide liability. Thus, the number of Class members is currently indeterminate, but is certainly numerous.

D. ADEQUACY OF REPRESENTATION

12. The Representative Plaintiff will fairly and adequately protect the interests of the class inasmuch as they are broadly representative, as reflected in the preceding paragraphs. There are no conflicts of interest present with the members of the proposed class as each would benefit from the imposition of a remedy for the Defendant's discriminatory employment practices. The Representative Plaintiff has retained counsel experienced in litigating major class actions in the field of employment discrimination, and who are prepared and able to meet the time and fiscal demands of class action litigation of this size and complexity. The combined interest, experience, and resources of the Representative Plaintiff and his counsel to litigate competently the individual and class claims of employment discrimination at issue satisfy the adequacy of representation requirement under Fed.R.Civ.P. 23(a)(4).

E. EFFICIENCY OF CLASS PROSECUTION OF COMMON CLAIMS

13. Certification of a class of similarly-situated applicants is the most efficient and economical means of resolving the questions of law and fact that are common to the individual claims of the Representative Plaintiff and the proposed class. The individual claim of the Representative Plaintiff requires resolution of the common question of whether Defendant has engaged in a systemic pattern of discrimination against African-Americans, those over forty (40) and the disabled. The Representative Plaintiff seeks remedies to undo the adverse effects of such discrimination in his own life and career. The Representative Plaintiff has standing to seek such relief because of the adverse effect that such discrimination has had on him individually and on the putative classes he seeks to represent, in general. In order to gain such relief for himself, as well as for the putative class members, the Representative Plaintiff will first establish the existence of systemic discrimination as the premise of the relief they seek. Without class certification, the same evidence and issues would be subject to re-litigation in a multitude of individual lawsuits with an attendant risk of inconsistent adjudications and conflicting obligations. Certification of the subclasses affected by the common questions of law and fact is the most efficient and judicious means of presenting the evidence and arguments necessary to resolve such questions for the Representative Plaintiff, the class and the Defendant. The Representative Plaintiff's individual and class claims are premised upon the traditional bifurcated method of proof and trial for systemic disparate treatment claims of the type at issue in this complaint. Such a bifurcated method of proof and trial is the most efficient method of resolving such common issues.

F. CERTIFICATION IS SOUGHT PURSUANT TO FED. R. CIV. P. 23(b)(2)

14. Workday has acted on grounds generally applicable to the Representative Plaintiff and the proposed class by adopting and following systemic practices and procedures that discriminate on the basis of race, age, and/or disability. Workday's screening products are regularly used to discriminate on the basis of race, age, and/or disability. Workday has refused to act on grounds generally applicable to the putative class by: (1) refusing to adopt or follow screening productions and selection procedures which do not systemically discriminate on the basis of race, age, and/or disability. Workday's discriminatory screening products have made appropriate final injunctive relief and declaratory relief with respect to the class as a whole. The injunctive relief and declaratory relief are the predominate reliefs sought because they are both the cumulation of the proof of the Defendant's individual and class-wide liability at the end of Stage I of a bifurcated trial and the essential predicate for the Representative Plaintiff and the class members entitlement to monetary and non-monetary remedies at Stage II of such a trial. Declaratory and injunctive relief flow directly and automatically from proof of the common questions of law and fact regarding the existence of systemic discrimination against individuals on the basis of race, age, and/or disability. Such relief is the factual and legal predicate for the Representative Plaintiff's and the class members entitlement to injunctive and equitable remedies caused by such systemic discrimination.

G. ALTERNATIVELY CERTIFICATION IS SOUGHT PURSUANT TO FED. R.CIV. P. 23(b)(3)

15. The common issues of fact and law affecting the claims of the Representative Plaintiff and proposed class members, including, but not limited to, the common issues identified above, predominate over any issues affecting only individual claims. A class action is superior to other available means for the fair and efficient adjudication of the claims of the Representative

Plaintiff and members of the proposed class. The cost of proving the Defendant's pattern or practice of discrimination makes it impracticable for the named Plaintiffs and members of the proposed class to control the prosecution of their claims individually. The Northern District of California is the most logical forum in which to litigate the claims of the Representative Plaintiff and the proposed class in this case because the Defendant's home office is here and it engages in or ratifies illegal conduct adversely affecting the Plaintiff here.

H. ALTERNATIVELY, CERTIFICATION IS SOUGHT PURSUANT TO FED. R. CIV. P. 23(c)(4) FOR INJUNCTIVE AND DECLARATORY RELIEF.

16. Alternatively, claims for injunctive and declaratory relief for the Injunctive Relief Class are properly certified under Federal Rule of Civil Procedure 23(c)(4) because such claims present only common issues, the resolution of which would advance the interests of the parties in an efficient manner.

I. ALTERNATIVELY, CERTIFICATION IS SOUGHT PURSUANT TO FED. R. CIV. P. 23(c)(4) FOR CLASS WIDE LIABILITY.

17. Alternatively, class wide liability claims are properly certified under Federal Rule of Civil Procedure 23(c)(4) for the Classes because such claims present only common issues, the resolution of which would advance the interests of the parties in an efficient manner.

J. PUNITIVE DAMAGES MAY ALTERNATIVELY BE CERTIFIED PURSUANT TO FED.R.CIV.P. 23(b)(2).

18. Punitive damages liability may alternatively be certified under Federal Rule of Civil Procedure 23(b)(2) because such relief focuses on the conduct of Workday and not the individual characteristics of the Plaintiff and are an allowable form of incidental monetary relief.

CLAIMS OF REPRESENTATIVE PLAINTIFF

Derek Mobley

19. Derek L. Mobley is an African-American male. He is over the age of forty (40) and suffers from anxiety and depression. Mr. Mobley was born in 1974.

20. Mr. Mobley is a graduate of Morehouse College in Atlanta, Georgia.

21. Founded in 1867, Morehouse College remains the only all-male Historically Black College or University in the world.

22. Graduates of Morehouse include Martin Luther King Jr., U.S. Senator Raphael Warnock, Shelton "Spike" Lee (award winning filmmaker), Samuel L. Jackson (award winning actor), and Jeh Charles Johnson (Obama Administration's Secretary of Homeland Security) to name a few.

23. Mr. Mobley graduated Morehouse in 1995 with a bachelor's degree in finance, cum laude.

24. Mr. Mobley is also an honors graduate of ITT Technical Institute. He is also Server+ Certified.

25. Since 2010, Mr. Mobley has worked in various financial, IT help-desk and customer service-oriented jobs.

26. Jobs and positions Mr. Mobley has occupied since graduating college include:

a. Capitol City Bank & Trust Company-Special Assets Manager/Commercial Credit Analyst;

b. Internal Revenue Service-Customer Service Representative;

c. AT&T Digital Life-Support Specialist, Level 1A Manager;

d. Bank of America-Card Services Collections Supervisor;

e. GE Capital-Floor Plan Account Manager;

f. DSD Mortgage, LLC-Owner and Manager Mortgage Company;

g. EAN Services, Inc. (Enterprise Rental Car)-Insurance Callbacks Representative;

h. Hewlett Packard Enterprise (HPE)-Advanced Solutions Engineer;

i. Uber Technologies-Contract Driver; and,

j. Allstate-Claims Dispatcher and Workflow Processor/Catastrophe Controller.

27. Mr. Mobley possesses extensive knowledge in multiple critical roles within the Enterprise server, banking, finance, and insurance industries.

How Algorithmic Discrimination Works

28. Defendant Workday unlawfully offers "algorithmic decision-making tools" that power applicant screening systems that in turn determine whether an employer should accept or reject an application for employment based on the individual's race, age, and or disability.

29. Today, discrimination is perpetuated through businesses seeking efficiencies by embracing automation and data mining. Employers use algorithmic models to quickly analyze large numbers of applications automatically based on given criteria such as keywords, skills, former employers, years of experience and schools attended ("data mining") to detect patterns and assist in making future decisions ("data analytics").

30. Data mining learns by example and accordingly what a model learns depends on the examples to which it has been exposed.[1] "Biased training data lead to discriminatory models."

[1] Solon Barocas and Andrew D. Selbst, *Big Data's Disparate Impact*, California Law Review Vol. 104, No. 3 (June 2016), pp. 671-732.

31. For hiring purposes data is mined on the front-end from applications via an Applicant Tracking System (“ATS), which can be located on the company’s website or extracted from applicants on job boards. An applicant tracking system (ATS) is a software application that enables the electronic handling of recruitment and hiring needs. Most job and resume boards (Reed Online, LinkedIn.com, Monster.com, Hotjobs, CareerBuilder, Indeed.com) have partnerships with ATS software providers to provide parsing support and easy data migration from one system to another.

32. Newer applicant tracking systems (often the epithet is next-generation) are platforms as a service, where the main piece of software has integration points that allow providers of other recruiting technology to plug in seamlessly. The ability of these next-generation ATS solutions allows jobs to be posted where the candidate is and not just on-job boards. This ability is being referred to as omnichannel talent acquisition.

33. So-called “machine-learning” algorithms are designed to learn based upon the algorithm’s access to a designated data set or an algorithm-driven search for data residing within an ATS.

34. Unfortunately, algorithms too often have discriminatory effects, even where demographic data such as race, age, and disability are not included as inputs. This is because algorithms can “learn” to use omitted demographic features by combining other inputs that are correlated with race (or another protected classification), like zip code, college attended, and membership in certain groups.

35. Moreover, if the data mined is based on the intentional prejudices or biases of prior trainers or a lack of diversity in the data set, data mining will learn from the unlawful example that these decisions furnish.

36. To illustrate, Amazon famously abandoned a facially neutral hiring algorithm in 2017 because of its disparate impact on female candidates. There, the training data presented to the algorithm consisted of resumes submitted to Amazon by applicants over a 10-year period, without presenting data to the algorithm explicitly indicating the applicants' gender. But most of these applicants were white males. Rather than sort candidates by qualifications or merit, the algorithm learned to favor male candidates by prioritizing language more commonly used by males, penalizing the word "women's" in resumes, and devaluing candidates who had graduated from all- women's colleges.

37. The algorithm simply drew inferences from a biased sample of the population (in the Amazon case all white males) and simply reproduced that prejudice which disadvantaged female applicants.

38. Upon information and belief, Workday determines which candidates to recommend based on the demonstrated interests of its client-employers in certain types of candidates, Workday will offer recommendations that reflect whatever biases employers happen to exhibit.

39. Upon information and belief, if Workday's algorithmic decision-making tools observe that a client-employer disfavors certain candidates who are members of a protected class, it will decrease the rate at which it recommends those candidates. Thus, the recommendation algorithmic decision-making tool caters to the prejudicial preferences of the client-employer.

40. Algorithmic decision-making and data analytics are not, and should not be assumed to be, race neutral, disability neutral, or age neutral. Too often, they reinforce and even exacerbate historical and existing discrimination.

41. For example, a 2019 study found that a clinical algorithm that many hospitals were using to determine which patients need care was biased: Black patients assigned the same level of risk—and thus allocated the same health care resources—were much sicker than white patients. This happened because the algorithm had been trained on historical health care spending data, which reflects a history in which Black patients had less money to spend on their health care than white patients. From this, the algorithm falsely concluded that Black patients were healthier than equally sick white patients.

42. Academics and government actors alike have cautioned that when approached without appropriate forethought and oversight, data analytics "can reproduce existing patterns of discrimination, inherit the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society. It can even have the perverse result of exacerbating existing inequalities by suggesting that historically disadvantaged groups actually deserve less favorable treatment."

43. Indeed, according to Federal Trade Center ("FTC") Commissioner Kelly Slaughter, "[i]n recent years, algorithmic decision-making has produced biased, discriminatory, and otherwise problematic outcomes in some of the most important areas of the American economy. These harms are often felt most acutely by historically disadvantaged populations, especially Black Americans and other communities of color." Interest in the susceptibility of data analytics and algorithmic decision-making to bias has become increasingly widespread.

44. For example, in 2022, the California Department of Insurance released the bulletin Allegations of Racial Bias and Unfair Discrimination in Marketing, Rating, Underwriting, and Claims Practices by the Insurance Industry, which declared that:

> "technology and algorithmic data are susceptible to misuse that results in bias, unfair discrimination, or other unconscionable impacts among similarly-situated

> consumers. A growing concern is the use of purportedly neutral individual characteristics as a proxy for prohibited characteristics that result in racial bias, unfair discrimination or disparate impact. The greater use by the insurance industry of artificial intelligence, algorithms, and other data collection models have resulted in an increase in consumer complaints relating to unfair discrimination in California and elsewhere. . . ."

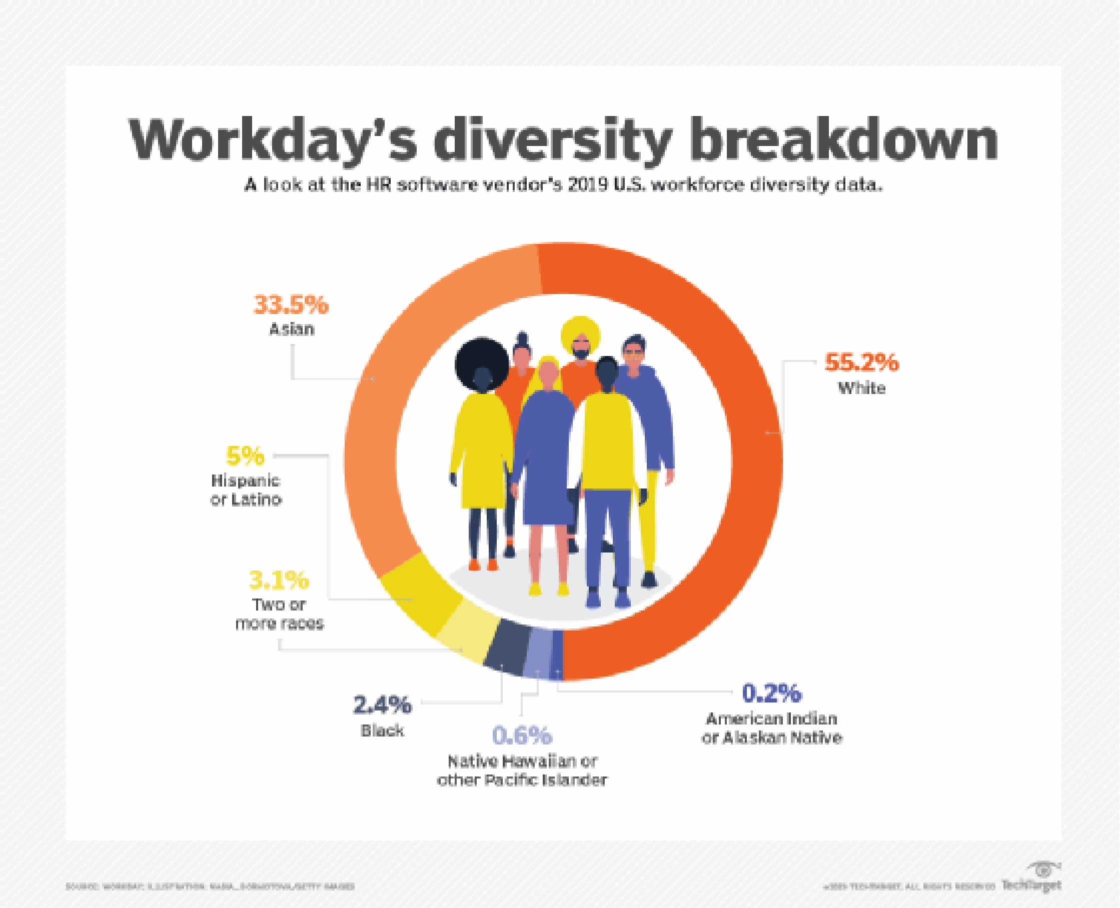
45. Upon information and belief, Workday's algorithmic decision-making tools lack sufficient guardrails to prevent discrimination. The conscious failure to include such guardrails is intentional and shows a reckless disregard for the anti-discrimination laws.

46. Further, lack of guardrails creates a phenomenon referred to as AI drift. AI drift occurs when an AI system's performance and behavior change over time, often due to the evolving nature of the data it interacts with and learns from. This can result in the Artificial intelligence system making predictions or decisions that deviate from its original design and intended purpose. "AI drift can perpetuate or amplify existing biases present in training data, leading to discriminatory or unfair outcomes. For instance, a hiring AI might start favoring certain demographics or perpetuating gender or racial biases" . . .i.e. disparate impact.[2]

47. Donald Tomaskovic-Devey, a sociology professor who heads the Center for Employment Equity commented as follows on Workday's diversity "Workday's website makes strong claims of corporate commitment to diversity, but at 2.4% Black, it is one of the poorest performing tech companies I have encountered."[3]

[2] https://www.analyticsinsight.net/what-is-ai-drift-and-the-risks-associated-with-it/

[3] https://www.techtarget.com/searchhrsoftware/news/252485468/Workday-admits-to-Black-diversity-problem-pledges-to-improve



[4]

48. Safiya Umoja Noble, Associate Professor, University of California, Los Angeles explained “The use of automated HR technologies has already shown many failings with respect to ensuring diversity -- and, in fact, many undermine it by screening out qualified women and perpetuating discrimination against African Americans who don't 'whiten' their resumes, who are often evaluated through software screening systems."[5] Limited diversity in the workforce responsible for creating models for training leads to bias in data mining which in turn leads to discriminatory and biased selection decisions.

[4] Id.

[5] Id.

Mobley's Applications

49. Since 2017, Mr. Mobley has applied for over 100 positions that exclusively use Workday, Inc. as a screening platform for talent acquisition and/or hiring. Each time he has been denied.

50. Workday is currently used by more than 10,000 organizations around the world and across industries—from medium-sized businesses to more than 50 percent of the Fortune 500.[6] The Workday customer community has 65 million users, and as of April 2023, nearly one in four of all U.S. job openings was processed on the Workday platform.

51. Mr. Mobley's application process generally began with him responding to a job advertisement or posting by a prospective employer on a third-party website such as LinkedIn, Indeed, Monster, or Careerbuilders.

52. Mr. Mobley then clicks on the job advertisement or posting link which directs him to the Workday platform on the employer's website.

53. For example, a job posting or advertisement link for Hewlett Packard Enterprise would say hpe@myworkday.com.

54. Mr. Mobley would then be prompted by the Workday platform to create a username and password to access the employment opportunity.

55. After creating a username and password, Mr. Mobley would then upload his resume` or enter his information manually. Mr. Mobley's resume` includes his graduation from Morehouse, a leading Historically Black College or University, and shows his extensive employment history which could be assessed as a proxy for age.

[6] https://newsroom.workday.com/company-overview

56. Numerous positions for which Mr. Mobley applied required him to take a Workday branded assessment and/or personality test.

57. Upon information and belief, these assessments and personality tests are unlawful disability related inquiries designed to identify mental health disorders or cognitive impairments and have no bearing on whether Mr. Mobley would be a successful employee.

58. These assessments and personality tests are likely to reveal mental health disorders and cognitive impairments and test for characteristics that correlate with them.

59. Persons with these disorders and impairments are likely to perform worse on these assessments and tests and be screened out. Mobley suffers from depression and anxiety.

60. Upon information and belief, these tests are “disability inquiries” and/or “medical examinations” in that they are designed to reveal mental-health disorders such as excessive anxiety, depression, and certain cognitive impairments.

61. In September 2017, Mr. Mobley applied for a position with Hewlett Packard Enterprise, a company for which he was already working on a contract basis, via hpe@myworkday.com.

62. His application was for a Service Solutions Technical Consultant’s position whose qualifications mirrored the position he occupied at the time.

63. On October 16, 2017, Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

64. In September 2018, Mr. Mobley applied for a Fraud Analyst position with Equifax, via equifax@myworkday.com.

65. On October 1, 2018, Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

66. On September 23, 2018, Mr. Mobley applied for a Corporate Travel Consultant's position with Expedia, via expedia@myworkday.com.

67. On October 2, 2018, at 2:19 a.m., Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

68. On March 31, 2019, Mr. Mobley applied for a Claim Support Representative's position with Fiserv, via fiserv@myworkday.com.

69. The very next morning, April 1, 2019, at 9:40 a.m., Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

70. In June 2019, Mr. Mobley applied for a Help Desk Support Technician with the NCR Corporation, via ncr@myworkday.com.

71. On June 20, 2019, Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

72. On August 31, 2019, Mr. Mobley applied for an Associate Customer Care Specialist position with Duke Energy, via dukeenergy@myworkday.com.

73. As part of the application process, Mr. Mobley was required to complete a Workday branded assessment for which he received no feedback.

74. Mr. Mobley was rejected for this position and was never notified as to why, even though he met its experiential and educational requirements.

75. Upon information and belief, the Workday branded assessment Mr. Mobley took was not "bias free" as claimed in its marketing materials.

76. Again, on August 31, 2019, Mr. Mobley applied for a Customer Service Representative position with Unum, via unum@myworkday.com.

77. That same day at 12:52 a.m., Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

78. On September 1, 2019, Mr. Mobley applied for a Purchase Specialist position with Quicken Loans, via the Quicken Loans Workday System quickenloans@myworkday.com.

79. On September 3, 2021, Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

80. On March 25, 2021, Mr. Mobley applied for a Service Center Representative position with Sedgwick, via sedgwick@workday.com.

81. On April 6, 2021, Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

82. On April 1, 2021, Mr. Mobley applied for a Virtual Telesales Representative position with Comcast, via comcast@myworkday.com.

83. On April 12, 2021, Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

84. On January 29, 2022, at 12:55 a.m., Mr. Mobley applied for a Customer Services Specialist [Full-time or Part-time & remote working] with Unum, via unum@myworkday.com.

85. Less than one-hour later [1:50 a.m.], Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements. Clearly, Mobley's applications are being processed by Workday's algorithmic decision-making tools.

86. On January 9, 2024, Mr. Mobley applied for a Customer Support Representative position with ResMed, via resmed@myworkday.com.

87. On January 11, 2024, at 3:52 a.m., Mr. Mobley was notified of his rejection for this position via email, even though he met its experiential and educational requirements.

88. Despite being qualified, and in many instances over-qualified, Mr. Mobley has not been successful at securing employment with any employer that uses the Workday platform as a screening tool for applicants.

89. Mr. Mobley has applied to firms that form Workday's core business which is medium-sized and large, global organizations that span numerous industry categories, including professional and business services, financial services, healthcare, education, insurance, government, technology, media, retail, and hospitality.

Workday is an Employment Agency

90. Firms purchase a subscription for Workday's services and as part of their subscription, customers are provided support services, including professional consulting, to enable them to delegate their human resource hiring function to the Workday platform.

91. Workday acts as an agent on behalf of the employers, who have delegated their employment hiring decision-making authority to it.

92. Acting expressly or impliedly and at the direction of employers, Workday denied Mr. Mobley and the putative class members employment unless they participated in the Workday platform. The Workday platform is the only way to gain employment with these employers.

93. Workday's subscription-based service reflects an on-going relationship with their client-employers and includes significant engagement in the process of hiring employees.

94. Workday's website states that it can "reduce time to hire by automatically dispositioning or moving candidates forward in the recruiting process."

95. In what it terms "Talent Management" Workday's systems source candidates and then use algorithmic decision-making tools to recommend job opportunities.

96. Workday's marketing materials state that "[a]dditionally, we offer extensive customer training opportunities and a professional services ecosystem of experienced Workday consultants and system integrators to help customers not only achieve a timely adoption of Workday but continue to get value out of our applications over the life of their subscription."

97. Workday's relationships with its client-employers are not one-off transactions but ongoing business arrangements where employers delegate their hiring function Workday who in turn uses its algorithmic decision-making tools to screen out applicants who are African-American, disabled, and/or over the age of 40.

98. As stated previously, a prospective employee can only advance in the hiring process if they get past the Workday platforms screening algorithms.

99. Workday embeds artificial intelligence ("AI") and machine learning ("ML") into its algorithmic decision-making tools, enabling these applications to make hiring decisions.

100. Workday's AI and ML also enables incumbent employees at firms to participate in the talent acquisition process by making referrals and recommendations. Workday does this by integrating pymetrics into its algorithmic decision-making tools for applicant screening.

101. The pymetrics Workday Assessment Connector is supposed to use neuroscience data and AI to help client-employers make their hiring and internal mobility decisions more predictive, and free of bias.

102. Upon information and belief, these algorithms are only trained on incumbent employees at a company, allowing the pymetrics Workday Assessment Connector to build a homogenous workforce not representative of the applicant pool.

103. Similarly, Workday also encourages and uses the recommendations of incumbent employees for hiring decisions. Upon information and belief, this facially neutral employment practice has a differential effect upon African-Americans, the disabled, and workers over the 40, because any lack of work force diversity allows for incumbent employees to consciously or unconsciously refer or recommend few, if any members of these protected classes.

104. These systems of recruiting new workers operate to discriminate against African-Americans, workers over the age of 40, and the disabled because they lock in the status quo.

105. A wealth of literature discusses the potential for bias resulting from algorithmic decision-making. As the FTC has acknowledged, algorithmic bias is everywhere. Mounting evidence reveals that algorithmic decisions can produce biased, discriminatory, and unfair outcomes in a variety of high-stakes economic spheres including employment, credit, health care, and housing.

106. In the housing context in particular, tools infected with bias are integrated into home financing, leasing, marketing, sales, and zoning decisions. For example, a 2021 report analyzing more than 2 million conventional mortgage applications found that lenders who processed applicants through Fannie Mae and Freddie Mac's FICO algorithms were 80% more likely to reject Black applicants than financially equivalent white applicants.

Workday Acts as an Agent

107. Using their "AI", "ML", assessments, tests, and pymetrics to make job recommendations (algorithmic decision-making tools) or control access to jobs (equitable or otherwise), makes Workday an agent for its client-employers.

108. Client-employers delegate to Workday certain aspects of the employers' selection decisions as to Mobley and the putative Class Members.

109. Chief among those was the decision to screen out Class Members from gaining employment.

110. Employers directed job applicants to the Workday job screening platform which then determines if they receive a job.

111. According to Workday's Marketing Materials, "Our skills intelligence foundation helps you build diverse teams by expanding candidate pools with equitable, AI- and ML-driven job recommendations."[7]

112. Disposing of candidates "en masse" through the use of algorithmic decision-making tools delegates to Workday the responsibility to oversee the applicant hiring process.

113. This process is the only means an employee who applies for a job with an employer who uses the Workday platform can obtain employment.

114. Workday is contracted to provide these services.

Workday is an Indirect Employer

115. Workday's ability to limit the employment opportunities of Mobley and the putative Class Members directly interferes with any direct employment relationship between them and prospective employers.

116. Workday's client contracts with them to provide these services via their algorithmic screening tools.

117. Workday is an indirect employer by virtue of its ability to discriminatorily interfere and exert peculiar control over the prospective employee's relationship with the direct employer.

[7] https://www.workday.com/en-us/products/talent-management/talent-acquisition.html

Challenged Discriminatory Practices

118. Mr. Mobley is challenging the use of these common discriminatory screening tools per se, and not merely the individualized manifestations of their use, the fact that the common components may vary to some small degree or be applied by different customers is of no consequence.

119. Individuals impacted the same way by these processes number in the thousands if not tens of thousands.

120. The selection tools, assessments, and/or tests utilized by Workday, Inc. in making selection decisions-to include screening and hiring applicants discriminate on the basis of race in violation of §703(k) of Title VII, 42 U.S.C. §2000e-2(k).

121. Upon information and belief, these processes disparately impact African-American applicants because they have the effect of disproportionately excluding African-Americans from jobs.

122. Furthermore, these selection procedures are not job-related, nor are they consistent with any business necessity.

123. Title VII prohibits discrimination by employment agencies. Section 703(b) of the Act, 42 U.S.C. § 2000e-2(b), reads: "it shall be an unlawful employment practice for an employment agency to fail or refuse to refer for employment, or otherwise to discriminate against, any individual because of his race, color, religion, sex, or national origin, or to classify or refer for employment any individual on the basis of his race, color, religion, sex, or national origin. Section 701(c) of the Act, 42 U.S.C. § 2000e(c), defines the term "employment agency" as: any person regularly undertaking with or without compensation to procure employees for an

employer or to procure for employees opportunities to work for an employer and includes an agent of such a person.

124. Workday, Inc. is an employment agency as that term is defined by Title VII because employers delegate to them the authority to act on the employer's behalf and rely on Workday's recommendation on whom to hire.

125. Upon information and belief, Mr. Mobley and other African-Americans have been intentionally discriminated against because of their race (African-American), in violation of Title VII Civil Rights Act of 1964, as amended.

126. Furthermore, the screening tools, to include assessments and tests, marketed by Workday for the administration of its products discriminate on the basis of disability in violation of the ADA Amendments Act of 2008 (ADAAA).

127. Upon information and belief, these screening tools disparately impact disabled applicants because they have the effect of disproportionately excluding individuals with disabilities. Furthermore, the screening tools are not job-related, nor are they consistent with any business necessity.

128. Finally, the screening tools marketed by Workday for hiring applicants discriminate on the basis of age in violation of the Age Discrimination in Employment Act of 1967 (ADEA).

129. Upon information and belief, these screening tools disparately impact applicants over the age of 40 because the assessments and/or tests have the effect of disproportionately excluding them. Furthermore, they are not job-related, nor are they consistent with any business necessity.

CLASS CLAIMS

COUNT ONE

Intentional Employment Discrimination in Violation of Title VII of the Civil Rights Act of 1964

130. Representative Plaintiff restates and incorporates by reference all applicable paragraphs above as part of this Count of Complaint.

131. Workday as an employment agency, agent, and/or indirect employer has intentionally discriminated against the Representative Plaintiff and the class he seeks to represent with regards to selection procedures and other terms and conditions of employment because of their race, African-American, in violation of Title VII of the Civil Rights Act of 1964.

132. Workday's conduct has been intentional, deliberate, willful and conducted with disregard for the rights of the Plaintiff and members of the proposed class.

133. By reason of Workday's discriminatory employment practices, the Representative Plaintiff and the proposed class members have experienced extreme harm, including loss of compensation, wages, back and front pay, and other employment benefits, and, as such, are entitled to all legal and equitable remedies available under Title VII of the Civil Rights Act of 1964.

134. Employers have delegated to Workday the decision to either permit or withhold Class Members from gaining employment. Prospective applicants cannot gain employment without accessing the Workday platform.

135. Workday utilizes "AI", "ML", assessments, tests and other screening tools in a discriminatory fashion that blocks African-American applicants from employment opportunities.

136. Workday has also interfered with the present and future employment prospects of class members that have used its application platform in violation of Title VII.

137. In the absence of a direct employment relationship Workday can still be held liable under Title VII for its discriminatory treatment of the class members because it has interfered with their opportunity to gain employment.

COUNT TWO

Disparate Impact Discrimination on the Basis of Race and Disability in Violation of Title VII of the Civil Rights Act of 1964, and the ADA Amendments Act of 2008.

138. Representative Plaintiff restates and incorporates by reference all applicable paragraphs above as part of this Count of the Complaint.

139. The algorithmic decision-making tools that Workday uses to screen out African-American and disabled applicants make it an employment agency under Title VII and the ADA. For purposes of these statutes, Workday is also an agent and/or indirect employer because (1) it has been delegated authority to make hiring decisions by direct employers and (2) it has the ability to interfere with and control access to employment opportunities with direct employers.

140. Workday as an employment agency, agent, and/or indirect employer utilizes discriminatory screening tools that consciously or unconsciously discriminate against applicants on the basis of race and/or disability. There is no business necessity justifying the disparate impact these screening tools have on individuals in these protected categories.

141. Because there are no guardrails to regulate Workday’s conduct, the algorithmic decision-making tools it utilizes to screen out applicants provide a ready mechanism for discrimination.

142. Workday’s algorithmic decision-making screen out tools discriminated against the Representative Plaintiff and the proposed class both within and outside the liability period in this case.

143. As a direct result of Workday's discriminatory screening tools as described above, the Representative Plaintiff and the class he seeks to represent have suffered damages including, but not limited to, lost past and future income, compensation, and benefits.

144. Workday has also interfered with the present and future employment prospects of class members that have used its application platform in violation of Title VII and the ADA.

145. In the absence of a direct employment relationship Workday can still be held liable under Title VII and the ADA for its discriminatory treatment of the class members because it has interfered with their opportunity to gain employment.

COUNT THREE

Intentional Discrimination
Age Discrimination in Employment Act of 1967, 29 U.S.C. §§ 623(a)(1)

146. Representative Plaintiff restates and incorporates by reference all applicable paragraphs above as part of this Count of the Complaint.

147. This claim is brought by the Representative Plaintiff on behalf of himself and the collective he seeks to represent.

148. Employers delegated hiring decisions to Workday who then, upon information and belief, utilized algorithmic decision-making tools that screened out applicants on the basis of age. For purposes of the ADEA, Workday is also an agent and/or indirect employer because (1) it has been delegated authority to make hiring decisions by direct employers and (2) it has the ability to interfere with and control access to employment opportunities with direct employers.

149. Workday intentionally utilized algorithmic decision-making tools to screen out the Representative Plaintiff and the collective on the basis of age in violation of the ADEA.

150. The discriminatory conduct that constitutes Workday's pattern and/or practice of discrimination have occurred both within and outside the liability period in this case.

151. As a direct result of Workday's intentional utilization of discriminatory algorithmic decision-making tools as described above, the Representative Plaintiff and the collective have suffered damages including, but not limited to, lost past and future income, compensation, and benefits.

152. The foregoing conduct constitutes illegal, intentional discrimination and unjustified disparate treatment prohibited by 29 U.S.C. § 623(a)(1).

COUNT FOUR

Disparate Impact Discrimination
Age Discrimination in Employment Act of 1967, 29 U.S.C. §§ 623(a)(2)

153. Representative Plaintiff restates and incorporates by reference all applicable paragraphs above as part of this Count of the Complaint.

154. This Claim is brought by Representative Plaintiff on behalf of himself and the collective he seeks to represent. Workday maintains discriminatory policies, patterns, and/or practices that have an adverse impact on employees ages 40 and older in violation of the ADEA and are not, and cannot be, justified by reasonable factors other than age.

155. Employers have delegated hiring decisions to Workday who then, upon information and belief, utilize discriminatory algorithmic decision-making tools that consciously or unconsciously discriminate against applicants on the basis of age. For purposes of the ADEA, Workday is also an agent and/or indirect employer because (1) it has been delegated authority to make hiring decisions by direct employers and (2) it has the ability to interfere with and control access to employment opportunities with direct employers.

156. There is no business necessity justifying the disparate impact these screen out tools have on individuals in this protected category.

157. Workday used discriminatory algorithmic decision-making tools both within and outside the liability period in this case.

158. As a direct result of Workday's discriminatory policies and/or practices as described above, the Representative Plaintiff and the collective he seeks to represent have suffered damages including, but not limited to, lost past and future income, compensation, and benefits.

COUNT FIVE

Intentional Discrimination
42 U.S.C. § 1981

159. Representative Plaintiff restates and incorporates by reference all applicable paragraphs above as part of this Count of Complaint.

160. Workday as an employment agency, agent, and/or indirect employer has intentionally discriminated against the Representative Plaintiff and the class he seeks to represent with regards to selection procedures and other terms and conditions of employment because of their race, African-American, in violation of 42 U.S.C. § 1981.

161. Workday's conduct has been intentional, deliberate, willful and conducted with disregard for the rights of the Plaintiff and members of the proposed class.

162. By reason of Workday's discriminatory employment practices, the Representative Plaintiff and the proposed class members have experienced extreme harm, including loss of compensation, wages, back and front pay, and other employment benefits, and, as such, are entitled to all legal and equitable remedies available under 42 U.S.C. § 1981.

163. Employers have delegated to Workday the decision to either permit or withhold Class Members from gaining employment. Prospective applicants cannot gain employment without accessing the Workday platform.

164. Workday utilizes “AI”, “ML”, assessments, tests and other screening tools in a discriminatory fashion that blocks African-American applicants from employment opportunities.

165. Workday has also interfered with the present and future employment prospects of class members that have used its application platform in violation of 42 U.S.C. § 1981.

166. In the absence of a direct employment relationship Workday can still be held liable under 42 U.S.C. § 1981 for its discriminatory treatment of the class members because it has interfered with their opportunity to gain employment.

COUNT SIX

Aiding and Abetting Race, Disability, and Age Discrimination
Cal. Gov. Code §12940(I)

167. Representative Plaintiff restates and incorporates by reference all applicable paragraphs above as part of this Count of Complaint.

168. In perpetrating the abovementioned actions and omissions, Workday as employment agency, agent, or indirect employer engaged in a pattern and practice of unlawful aiding and abetting of discrimination in violation of California’s Fair Employment and Housing Act, Cal. Gov. Code §12940(i).

169. Workday attempted to and did in fact, aid, abet, incite, compel, and/or coerce their client-customers to engage in unlawful race, disability, and age discrimination the class members as described above.

170. As a direct and proximate result of the aforesaid discrimination based on race, disability, and age, the class members have sustained injury in the form of severe emotional

distress, humiliation, embarrassment, and mental anguish, all to their damage in an amount according to proof.

171. Workday's acts were wanton, willful and intentional, and were committed with malicious and reckless disregard for the rights and sensibilities of the class members.

PRAYER FOR RELIEF

WHEREFORE, the Representative Plaintiff and the Proposed Classes pray for relief as follow:

1. Certification of the case as a class action on behalf the proposed subclasses;

2. Designation of Plaintiff as representative of the subclasses;

3. Designation of Plaintiff's Counsel of record as Class Counsel;

4. A declaratory judgment that the practices complained of herein are unlawful and violate Title VII, 42 U.S.C. § 1981, the ADEA, the ADAAA, and Cal. Gov. Code §12940(I);

5. A preliminary and permanent injunction against the Company and its officers, agent, successors employees, representatives, and any and all persons acting in correct with them from engaging in each of the unlawful policies, practices, customs, and usages set forth herein;

6. An order that the Company institute and carry out policies, practices, and programs that provide equal employment opportunities for all minorities, and that it eradicate the effects of its past and present unlawful employment practices;

7. For back pay, front pay and other monetary relief according to proof (including interest and benefits);

8. For all damages sustained as a result of the Company's conduct according to proof;

9. For compensatory damages, nominal damages, and liquidated damages according to proof;

10. For exemplary and punitive damages in an amount commensurate with the Company's ability to pay, to deter future conduct, and to set an example for others;

11. For reasonable attorneys' fees and cost including under to the extent allowable by law;

12. Pre-judgment and post-judgment interest, as provided by law;

13. For such ancillary orders, decrees and such further legal and equitable relief as may be necessary to enjoin and restrain the improper conduct and wrongdoing of Defendant; and

14. For such other and further relief as the Court deems proper.

JURY TRIAL DEMANDED

Respectfully submitted,

/s/Roderick T. Cooks

/s/Lee D. Winston

Lee D. Winston
Roderick T. Cooks
Attorneys for the Plaintiffs and Proposed
Classes and Collective Members

OF COUNSEL:
Lee D. Winston
lwinston@winstoncooks.com
Roderick T. Cooks
rcooks@winstoncooks.com
Winston Cooks, LLC
420 20th Street North
Suite 2200
Birmingham, AL 35203
Telephone: (205) 502-0970
Facsimile: (205) 278-5876

LOCAL COUNSEL:
Jay Greene
Greene Estate, Probate, and Elder Law Firm
447 Sutter Street, Suite 435
San Francisco, CA 94108
Phone 415-905-0215
greeneattorney@gmail.com

CERTIFICATE OF SERVICE

I hereby certify that on **February 20th, 2024**, I electronically filed the foregoing document with the United States District Court for the Northern District of California by using the CM/ECF system. I certify that the following parties or their counsel of record are registered as ECF Filers and that they will be served by the CM/ECF system:

Erin M. Connell	econnell@orrick.com
Jay Patrick Greene	jay@jaygreenelawfirm.com
Julie Ann Totten	jtotten@orrick.com, jponce@orrick.com
Justin Washington	justin.washington@orrick.com
Kayla Delgado Grundy	kgrundy@orrick.com

s/Roderick T. Cooks
Of Counsel

OFFICE OF THE GENERAL COUNSEL

MEMORANDUM GC 23-02 **October 31, 2022**

TO: All Regional Directors, Officers-in-Charge,
and Resident Officers

FROM: Jennifer A. Abruzzo, General Counsel

SUBJECT: Electronic Monitoring and Algorithmic Management of Employees
Interfering with the Exercise of Section 7 Rights

Recent technological advances have dramatically expanded employers' ability to monitor and manage employees within the workplace and beyond. As more and more employers take advantage of those new capabilities, their practices raise a number of issues under the Act. An issue of particular concern to me is the potential for omnipresent surveillance and other algorithmic-management tools to interfere with the exercise of Section 7 rights by significantly impairing or negating employees' ability to engage in protected activity and keep that activity confidential from their employer, if they so choose.[1] Thus, I plan to urge the Board to apply the Act to protect employees, to the greatest extent possible, from intrusive or abusive electronic monitoring and automated management practices that would have a tendency to interfere with Section 7 rights. I will do so both by vigorously enforcing extant law and by urging the Board to apply settled labor-law principles in new ways, as described below.

It is well documented that employers are increasingly using new technologies to closely monitor and manage employees.[2] In warehouses, for example, some employers record

[1] In this memorandum, I use the term "automated management" or "algorithmic management" to refer to "a diverse set of technological tools and techniques to remotely manage workforces, relying on data collection and surveillance of workers to enable automated or semi-automated decision-making." Alexandra Mateescu & Aiha Nguyen, *Explainer: Algorithmic Management in the Workplace*, Data & Society Research Institute (Feb. 2019), *available at* https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf.

[2] Danielle Abril, *Your Boss Can Monitor Your Activities Without Special Software*, Washington Post (Oct. 7, 2022), *available at* https://www.washingtonpost.com/technology/2022/10/07/work-app-surveillance/; Jo Constantz, *"They Were Spying On Us": Amazon, Walmart, Use Surveillance Technology to Bust Unions*, Newsweek (Dec. 13, 2021), *available at* https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillance-technology-bust-unions-1658603; Richard A. Bales & Katherine V. W. Stone, *The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace*, 41 Berkeley J. Emp. & Lab. L. 1, 16-22 (2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3410655; Charlotte Garden, *Labor*

workers' conversations and track their movements using wearable devices, security cameras, and radio-frequency identification badges.[3] On the road, some employers keep tabs on drivers using GPS tracking devices and cameras.[4] And some employers monitor employees who work on computers—whether in call centers, offices, or at home—using keyloggers and software that takes screenshots, webcam photos, or audio recordings throughout the day.[5]

Electronic monitoring and automated management are not always limited to working time. After the workday ends, some employers continue to track employees' whereabouts and communications using employer-issued phones or wearable devices, or apps installed on workers' own devices.[6] And even before the employment relationship begins, some employers pry into job applicants' private lives by conducting personality tests and scrutinizing applicants' social media accounts.[7]

Importantly, advances in artificial intelligence and algorithm-based decision-making in recent years have made it possible for employers to analyze, sell or otherwise share, and act on the voluminous data that new technologies generate.[8] Some employers use that

Organizing in the Age of Surveillance, 63 St. Louis U. L.J. 55, 56-57 (2018), *available at* https://scholarship.law.slu.edu/lj/vol63/iss1/5/. *See also* Kate Bronfenbrenner, Testimony before the United States House Committee on Education and Labor, *In Solidarity: Removing Barriers to Organizing*, Cornell School of Indus. and Labor Relations, at 11-12 (Sept. 14, 2022), *available at* https://ecommons.cornell.edu/handle/1813/111838 (noting increase in electronic surveillance during union campaigns).

[3] Bales & Stone, *supra*, at 17, 20; Garden, *supra*, at 57.

[4] Kathryn Zickuhr, *Workplace Surveillance Is Becoming the New Normal for U.S. Workers*, Wash. Ctr. for Equitable Growth, at 4 (Aug. 2021), *available at* https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/.

[5] Garden, *supra*, at 56. *See* Letter from Rep. Robert "Bobby" Scott, Chairman, Committee on Education and Labor, U.S. House of Representatives, to Gene Dodaro, Comptroller, GAO (Oct. 5, 2022), *available at* https://edlabor.house.gov/download/scott-letter-to-gao-re-bossware (discussing "bossware" technology used to monitor employees in telework and office settings).

[6] *See* Emma Oppenheim, *Shining a Spotlight on Workers' Financial Experiences*, CFPB (Mar. 9, 2022), *available at* https://www.consumerfinance.gov/about-us/blog/shining-a-spotlight-on-workers-financial-experiences/; Bales & Stone, *supra*, at 20-22.

[7] Bales & Stone, *supra*, at 10-15.

[8] *Id.*; *Policy Statement on Enforcement Related to Gig Work*, FTC, at 10 (Sept. 15, 2022), *available at* https://www.ftc.gov/legal-library/browse/policy-statement-enforcement-related-gig-work.

data to manage employee productivity, including disciplining employees who fall short of quotas, penalizing employees for taking leave, and providing individualized directives throughout the workday.[9]

Under settled Board law, numerous practices employers may engage in using new surveillance and management technologies are already unlawful. In cases involving employer observation of open protected concerted activity and public union activity like picketing or handbilling, the Board has recognized that "pictorial recordkeeping tends to create fear among employees of future reprisals."[10] The Board accordingly balances an employer's justification for surveillance "against the tendency of that conduct to interfere with employees' right to engage in concerted activity."[11] In that context, "the Board has long held that absent proper justification, the photographing of employees engaged in protected concerted activities violates the Act because it has a tendency to intimidate."[12]

In addition, it is well established that an employer violates Section 8(a)(1) if it institutes new monitoring technologies in response to activity protected by Section 7; utilizes technologies already in place for the purpose of discovering that activity, including by reviewing security-camera footage or employees' social-media accounts; or creates the impression that it is doing such things.[13] Employer surveillance of Section 7 activity is

[9] Annette Bernhardt, Lisa Kresge & Reem Suleiman, *Data & Algorithms at Work: The Case for Worker Technology Rights*, UC Berkeley Labor Center, at 6 (Nov. 2021), *available at* https://laborcenter.berkeley.edu/data-algorithms-at-work/; Jodi Kantor, Karen Weise & Grace Ashford, *The Amazon That Customers Don't See*, New York Times (June 15, 2021), *available at* https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html; Zickuhr, *supra*, at 20; Bales & Stone, *supra*, at 17-18. Although the trend is visible across the national economy, the rising use of intrusive monitoring and management technologies disproportionately affects low-wage workers, workers of color, immigrants, and women, who are more likely to work in heavily tracked positions in warehousing, package delivery, and call centers. Bernhardt, Kresge & Suleiman, *supra*, at 15; Zickuhr, *supra*, at 12.

[10] *Brasfield & Gorrie, LLC*, 366 NLRB No. 82, slip op. at 5 (2018) (quoting *National Steel & Shipbuilding Co.,* 324 NLRB 499, 499 (1997), *petition for review denied,* 156 F.3d 1268 (D.C. Cir. 1998)).

[11] *F.W. Woolworth Co.*, 310 NLRB 1197, 1197 (1993) (citations and internal quotation marks omitted).

[12] *Id.*

[13] *See, e.g.*, *National Captioning Institute*, 368 NLRB No. 105, slip op. at 5 ("It is well settled that an employer commits unlawful surveillance if it acts in a way that is out of the ordinary in order to observe union activity."); *AdvancePierre Foods, Inc.*, 366 NLRB No. 133, slip op. at 2 n.4, 15-16 (2018) (employer's review of break-room security-camera footage to observe employee distribution of union literature was unlawful

unlawful whether it is carried out openly or covertly[14] and certain conduct can be unlawful even if it merely creates an impression of surveillance.[15] An employer who spends money on surveillance technology "to obtain information concerning the activities of employees or a labor organization in connection with a labor dispute involving such employer," or otherwise expends money to interfere with, restrain, or coerce employees in the exercise of the right to organize and bargain collectively through representatives of their own choosing, must generally file a Form LM-10, reporting the expenditure to the U.S. Department of Labor's Office of Labor-Management Standards.[16]

It is clear under extant law that employers violate Section 8(a)(1) if they discipline employees who concertedly protest workplace surveillance or the pace of work set by algorithmic management.[17] Employers also violate Section 8(a)(1) if they coercively question employees with personality tests designed to evaluate their propensity to seek

surveillance), *enforced*, 966 F.3d 813 (D.C. Cir. 2020); *National Captioning Institute, Inc.*, 368 NLRB No. 105, slip op. at 5 (2019) ("intentional monitoring of pro-union employees' Facebook postings" violates the Act); *Mek Arden, LLC*, 365 NLRB No. 109, slip op. at 19 (2017) (employer unlawfully created impression of surveillance by stating that voice-activated security cameras were monitoring union activity), *enforced*, 755 F. App'x 12 (D.C. Cir. 2018).

[14] *NLRB v. Grower-Shipper Vegetable Ass'n*, 122 F.2d 368, 376 (9th Cir. 1941).

[15] *Frontier Telephone of Rochester, Inc.*, 344 NLRB 1270, 1276 (2005) ("In determining whether an employer has unlawfully created the impression of surveillance of employees' union activities, the test that the Board has applied is whether, under all the relevant circumstances, reasonable employees would assume from the statement in question that their union or other protected activities had been placed under surveillance."), *enforced*, 181 F. App'x 85 (2d Cir. 2006).

[16] 29 USC § 433(a)(3). *See* OLMS Fact Sheet, Form LM-10 Employer Reporting: Transparency Concerning Persuader, Surveillance, and Unfair Labor Practice Expenditures, at 3, *available at* https://www.dol.gov/sites/dolgov/files/OLMS/regs/compliance/LM10_FactSheet.pdf (describing obligation to report expenditures on "[s]urveillance equipment or other technology used to surveil and the time spent on installing, operating, and monitoring it, as well as analyzing the information the equipment produces" among others). OLMS relies on Board findings in enforcing these reporting requirements. To promote compliance in cases that do not proceed to a Board decision, Regions should add the following language to settlement proposals in appropriate cases: "The Charged Party will report to the U.S. Department of Labor, Office of Labor-Management Standards, via its Form LM-10, the amount of any payments or expenditures made in conjunction with the conduct at issue in this case."

[17] *See NLRB v. Wash. Aluminum Co.*, 370 U.S. 9, 15 (1962) (employees' walkout to protest working conditions was protected); *Accel, Inc.*, 339 NLRB 1052, 1052 (2003) (employer unlawfully discharged employees for protesting requirement to work through a scheduled break).

union representation.[18] And employers violate Section 8(a)(1) if they dismantle or preclude employee conversations or isolate union supporters or discontented employees to prevent Section 7 activity.[19]

Further, if employers rely on artificial intelligence to screen job applicants or issue discipline, the employer—as well as a third-party software provider—may violate Section 8(a)(3) if the underlying algorithm is making decisions based on employees' protected activity.[20] Employers also violate Section 8(a)(3) by discriminatorily applying production quotas or efficiency standards to rid themselves of union supporters.[21] Finally, where employees have union representation, employers violate Section 8(a)(5) if they fail to provide information about, and bargain over, the implementation of tracking technologies and their use of the data they accumulate.[22]

In addition to zealously enforcing the foregoing precedent, I will urge the Board to adopt a new framework for protecting employees from intrusive or abusive forms of electronic monitoring and automated management that interfere with Section 7 activity. It is the Board's responsibility "to adapt the Act to changing patterns of industrial life."[23] An employer's right to oversee and manage its operations with new technologies is "not

[18] *See Facchina Construction, Co.*, 343 NLRB 886, 886 (2004) (employer violated the Act by questioning job applicant about union membership), *enforced*, 180 F. App'x 178 (D.C. Cir. 2006); *Allegheny Ludlum Corp.*, 333 NLRB 734, 740 (2001) (an employer engages in unlawful polling by forcing an employee to make "an observable choice that demonstrates their support for or rejection of the union"), *enforced*, 301 F.3d 167 (3d Cir. 2002).

[19] *See Trus Joist MacMillan*, 341 NLRB 369, 373 (2004) (employer violated Section 8(a)(1) by restricting employee's movements within facility during working time "to curtail employees' union discussions").

[20] *See Phelps Dodge Corp. v. NLRB*, 313 U.S. 177, 186-87 (1941) (discrimination in hiring against union supporters violates the Act); *Blankenship & Associates*, 306 NLRB 994, 995 (1992) (entering order against consultant acting as employer's agent).

[21] *See Roemer Industries*, 367 NLRB No. 133, slip op. at 17 (2019) (finding employer's claim that it discharged union supporter for inefficiency to be pretextual), *enforced*, 824 F. App'x 396 (6th Cir. 2020).

[22] *See Anheuser-Busch, Inc.*, 342 NLRB 560, 560 (2004) (employer violated the Act by failing to bargain with union prior to installation and use of surveillance cameras in the workplace), *enforced in pertinent part sub nom. Brewers & Maltsters, Local Union No. 6 v. NLRB*, 414 F.3d 36 (D.C. Cir. 2005). *See generally* Lisa Kresge, *Union Collective Bargaining Agreement Strategies in Response to Technology*, Working Paper, UC Berkeley Labor Center (Nov. 2020), *available at* https://laborcenter.berkeley.edu/wp-content/uploads/2022/01/Working-Paper-Union-Collective-Bargaining-Agreement-Strategies-in-Response-to-Technology-v2.pdf (discussing collective-bargaining-agreement provisions addressing employers' use of technology in the workplace).

[23] *NLRB v. J. Weingarten, Inc.*, 420 U.S. 251, 266 (1975).

unlimited in the sense that [it] can be exercised without regard to any duty which the existence of rights in others may place upon [the] employer."[24] Rather, it is up to the Board to work out an "adjustment" between the interests of management and labor that guarantees employees a meaningful "[o]pportunity to organize."[25] Consistent with the Board's statutory role, I will urge the Board to ensure that intrusive or abusive methods of electronic surveillance and automated management do not unlawfully interfere with, restrain, or coerce employees in the exercise of their Section 7 rights by stopping union and protected concerted activity in its tracks or preventing its initiation.[26]

The framework I will advocate is grounded in well-settled Board principles. The Board has held, with the Supreme Court's approval, that "the right of employees to self-organize and bargain collectively established by [Section 7] necessarily encompasses the right effectively to communicate with one another regarding self-organization at the jobsite."[27] The workplace "is the one place where employees clearly share common interests and where they traditionally seek to persuade fellow workers in matters affecting their union organizational life and other matters related to their status as employees."[28] Employers cannot lawfully prevent discussions about such matters, even during working time, if (as is often the case) they permit other kinds of non-work discussions.[29] And "time outside working hours, whether before or after work, or during luncheon or rest periods, is an employee's time to use as [the employee] wishes without unreasonable restraint, although the employee is on company property."[30]

In addition, both inside and outside of the workplace, "[t]he confidentiality interests of employees have long been an overriding concern to the Board."[31] Because employers so commonly retaliate against employees for exercising their Section 7 rights, the Board recognizes, with court approval, that a "right to privacy" is "necessary to full and free

[24] *Republic Aviation Corp. v. NLRB*, 324 U.S. 793, 798 (1945).

[25] *Id.*

[26] *Cf. Parexel International, LLC*, 356 NLRB 516, 519-20 (2011) (finding unlawful a "preemptive strike" discharge that prevented employees "from discussing, and possibly inquiring further or acting in response to, substandard wages or perceived wage discrimination").

[27] *Beth Israel Hosp. v. NLRB*, 437 U.S. 483, 491 (1978).

[28] *Eastex, Inc. v. NLRB*, 437 U.S. 556, 574 (1978) (quoting *Gale Products*, 142 NLRB 1246, 1249 (1963)) (brackets omitted).

[29] *Sysco Grand Rapids, LLC*, 367 NLRB No. 111, slip op. at 26 (2019), *enforced in pertinent part*, 825 F. App'x 348 (6th Cir. 2020).

[30] *Republic Aviation*, 324 U.S. at 803 n. 10 (1945) (quoting *Peyton Packing Co.*, 49 NLRB 828, 843 (1943)).

[31] *National Telephone Directory Corp.*, 319 NLRB 420, 421 (1995).

exercise of the organizational rights guaranteed by the [Act]."[32] The Board, accordingly, holds that "Section 7 of the Act gives employees the right to keep confidential their union activities,"[33] and it "zealously seeks to protect the confidentiality interests of employees."[34] In short, "employees should be free to participate in union organizing campaigns [or other protected concerted activity] without the fear that members of management are peering over their shoulders, taking note of who is involved in [Section 7] activities, and in what particular ways."[35]

Close, constant surveillance and management through electronic means threaten employees' basic ability to exercise their rights. In the workplace, electronic surveillance and the breakneck pace of work set by automated systems may severely limit or completely prevent employees from engaging in protected conversations about unionization or terms and conditions of employment that are a necessary precursor to group action.[36] If the surveillance extends to break times and nonwork areas, or if excessive workloads prevent workers from taking their breaks together or at all, they may be unable to engage in solicitation or distribution of union literature during nonworking time.[37] And surveillance reaching even beyond the workplace—or the use of technology that makes employees reasonably fear such far-reaching surveillance—may prevent employees from exercising their Section 7 rights anywhere.

I am mindful that some employers may have legitimate business reasons for using some forms of electronic monitoring and automated management. But to the extent that employers have a legitimate need to electronically monitor and direct employees in ways that could inhibit Section 7 activity, the employer's interests must be balanced against

[32] *Pac. Molasses Co. v. NLRB Reg'l Off. No. 15*, 577 F.2d 1172, 1182 (5th Cir. 1978).

[33] *Guess?, Inc.*, 339 NLRB 432, 434 (2003). *Accord Veritas Health Servs., Inc. v. NLRB*, 671 F.3d 1267, 1274 (D.C. Cir. 2012).

[34] *Wright Elec., Inc. v. NLRB*, 200 F.3d 1162, 1165 (8th Cir. 2000). *Accord United Nurses Ass'ns of Cal. v. NLRB*, 871 F.3d 767, 785 (9th Cir. 2017).

[35] *Flexsteel Industries*, 311 NLRB 257, 257 (1993).

[36] *See Alternative Energy Applications, Inc.*, 361 NLRB 1203, 1206 n.10 (2014) (noting that "discussions of wages are often preliminary to organizing or other action for mutual aid or protection"). *Cf. Spring Valley Hospital Medical Center*, 363 NLRB 1766, 1766 n.3, 1782 (2016) (adopting, in absence of exceptions, judge's finding that employer violated Section 8(a)(1) by requiring employees to speak English only, which limited employees' "ability to freely discuss and communicate about work conditions, wages and other terms and conditions of employment").

[37] *See Peyton Packing*, 49 NLRB at 843 (absent special circumstances, employers must allow their employees to engage in union solicitation on employer premises during nonwork time), *enforced*, 142 F.2d 1009 (5th Cir. 1944); *Stoddard-Quirk Manufacturing Co.*, 138 NLRB 615, 620 (1962) (employees generally may distribute union-related literature on their employer's premises, but the employer may restrict the distribution to nonwork areas).

employees' rights under the Act.[38] The Board must reach an accommodation between competing employer interests and employee rights "with as little destruction of one as is consistent with the maintenance of the other."[39]

Thus, in appropriate cases, I will urge the Board to find that an employer has presumptively violated Section 8(a)(1) where the employer's surveillance and management practices, viewed as a whole, would tend to interfere with or prevent a reasonable employee from engaging in activity protected by the Act. If the employer establishes that the practices at issue are narrowly tailored to address a legitimate business need—i.e., that its need cannot be met through means less damaging to employee rights—I will urge the Board to balance the respective interests of the employer and the employees to determine whether the Act permits the employer's practices. If the employer's business need outweighs employees' Section 7 rights, unless the employer demonstrates that special circumstances require covert use of the technologies, I will urge the Board to require the employer to disclose to employees the technologies it uses to monitor and manage them, its reasons for doing so, and how it is using the information it obtains. Only with that information can employees intelligently exercise their Section 7 rights and take appropriate measures to protect the confidentiality of their protected activity if they so choose.[40]

The foregoing framework is consistent with the approach I have advocated in cases where an employer maintains facially neutral work rules that could interfere with the exercise of Section 7 rights.[41] In those circumstances, as here, I have urged the Board to evaluate the effect of employer rules on a reasonable employee who is in a position of economic vulnerability, taking into account the totality of the surrounding circumstances.[42] And in doing so, I have urged the Board to give full consideration to employers' business needs, and to "permit[] employers to maintain narrowly tailored rules that infringe on employees' Section 7 rights in the limited circumstances where conflicting legitimate business interests outweigh those rights."[43] In the same way, with regard to investigative-confidentiality rules, I have urged the Board to permit restrictions on statutorily protected

[38] *See Guess?*, 339 NLRB at 434-35 (balancing employer's legitimate need for information against employees' Section 7 right to keep union activities confidential).

[39] *NLRB v. Babcock & Wilcox Co.*, 351 U.S. 105, 112 (1956).

[40] In addition, I will consider whether other safeguards or assurances are necessary to protect employees' Section 7 rights. *See, e.g.*, Garden, *supra*, at 67-68 (discussing proposals to require employers to limit who may access information obtained through electronic surveillance and algorithmic management, and to permit employees to respond before imposing discipline based on such information).

[41] *See generally Stericycle, Inc.*, Case Nos. 04-CA-137660 et al., Brief to the Board dated Mar. 7, 2022.

[42] *Id.* at 3, 12.

[43] *Id.* at 4, 13.

employee communications “only when legitimate and substantial justifications outweigh employees’ Section 7 rights in a particular investigation.”[44]

Finally, I note that I am committed to an interagency approach to these issues, as numerous agencies across the federal government are working to prevent employers from violating federal law using electronic surveillance and algorithmic management technologies. Through those efforts, agencies including the Federal Trade Commission, the Consumer Financial Protection Bureau, Department of Justice, Equal Employment Opportunity Commission, and the Department of Labor are working to combat a range of harms employers inflict on workers using such technologies, from discrimination in hiring and work assignments, to misclassification of employees as independent contractors, to other unfair or deceptive pay practices, to selling or sharing workers’ personal data, to injuries caused by overwork and repetitive motions.[45] Recent agreements that we have signed with many of these agencies will facilitate information sharing and coordinated enforcement on these issues.[46]

Consistent with the principles set forth above, Regions should vigorously enforce extant Board law in cases involving new workplace technologies. In addition, Regions should submit to Advice any cases involving intrusive or abusive electronic surveillance and algorithmic management that interferes with the exercise of Section 7 rights.

/s/
J.A.A.

[44] *Id.* at 16.

[45] *See* Press Release, Justice Department and EEOC Warn Against Disability Discrimination (May 12, 2022), *available at* https://www.justice.gov/opa/pr/justice-department-and-eeoc-warn-against-disability-discrimination (discussing technical assistance document concerning disability discrimination resulting from the use of artificial intelligence and algorithmic decision-making); FTC Policy Statement on Enforcement Related to Gig Work, *supra* (discussing FTC’s enforcement priorities in relation unfair and deceptive practices involving surveillance and algorithm-based decision-making, and exclusionary or predatory conduct by dominant firms that may unlawfully create or maintain a monopoly or a monopsony resulting poorer working conditions for gig workers); Oppenheim, *supra* (noting CFPB’s intention to closely monitor the collection and sale of workers’ data and assess where provisions of the Fair Credit Reporting Act and other consumer protection laws may protect workers).

[46] *See* NLRB Interagency Memoranda of Understanding, *available at* https://www.nlrb.gov/guidance/key-reference-materials/interagency-international-collaboration/interagency-MOUs.