The October 30, 2023 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence: Is It Making Your Intellectual Property More Secure?

By

Gary Rinkerman*

Abstract

The recent Biden White House Executive Order on artificial intelligence is a sweeping attempt to assess, monitor, regulate, and direct developments in this important area of technological growth. However, while the Order contemplates massive and thorough (arguably intrusive) collections of information, including information that will be trade secret and otherwise commercially valuable, it does not specifically address the issue of how better to ensure that government officials, employees, agents, and contractors have proper training to make sure that third-party proprietary rights in that information are preserved and the information is not "leaked" or otherwise improperly published by those acting under color of federal authority. In addition, while the Order seeks information to better assess the refusal by the U.S. Copyright Office and the U.S. Patent Office to afford protection to matter created wholly by artificial intelligence, there is a lack of specific direction on the potential need to alter these positions or focus on developing – at the federal or state levels – new forms of intellectual property protection for such matter.

Discussion

On October 30, 2023, the Biden White House issued an *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (the Order). [1] The Order is largely premised on the view that Artificial Intelligence (AI) urgently requires pervasive federal government inquiry, oversight, monitoring, and control to ensure that AI is properly developed and

* Gary Rinkerman is an attorney whose practice includes intellectual property litigation, transactions, and counseling. He is an Honorary Professor of U.S. Intellectual Property Law at Queen Mary University in London, UK and also a Senior Fellow at the Center for Assurance Research and Engineering ('CARE') in the College of Engineering and Computing at George Mason University in Virginia. For those interested in 'digital archeology,' Mr. Rinkerman, as a Senior Investigative Attorney for the U.S. International Trade Commission, successfully argued one of the first cases in which copyright in object code was enforced. He also co-founded and served as Editor-in-Chief for *Computer Law Reporter*, one of the first legal publications (in the 1980s) to focus exclusively on law and computer technologies. This article should not be considered legal advice. The presentation of facts and the opinions expressed in this discussion are attributable solely to the author and do not necessarily reflect the views of any firms, persons, organizations or entities with which he is affiliated or whom he represents.

[1] *See* https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (last accessed Dec. 29, 2023).

used in conformity with approved technological, industrial and societal goals.[2] Some readers will welcome the Order's broad and ambitious sweep, others will see the Order and its nuanced language as a political and policy driven overreach into a number of issues more properly addressed by Congress, the judiciary, and in agreements between private entities – or maybe just left alone. There is also in the Order a priority placed on "approved notions of equity and civil rights" which can be viewed as laudable by the optimistic or viewed by the cynical as biased against groups who have not yet obtained sufficient financial or political resources to defend themselves. However, this brief introductory discussion will focus on selected aspects of the Order that can have profound effects on intellectual property (IP) such as trade secrets, copyrights and patents. There are also very important IP sections in the Order regarding watermarking[3] to identify and validate content as well as a number of sections concerned with protecting against AI-related IP theft and enforcing AI-related IP rights.[4] These IP-related watermarking, risk mitigation, and enforcement provisions will be treated in a second installment of this discussion. Also, specific (arguable) biases and presumptions in the Order, as well as important national security concerns, cybersecurity, privacy, and other aspects of the Order, will be reserved for future discussion.

There are several sections of the Order that require government gathering and assessment of information that will necessarily include private entities' trade secret and confidential information. For example, the determinations of whether particular AI systems are appropriately secure and acceptably correct from a technological or policy standpoint, through *e.g.,* "AI red teaming,"[5] will likely or necessarily result in disclosure of commercially valuable data, algorithms, and analyses to officers, agents, and employees of the federal government as well as contractors working with the federal government. Notwithstanding the concern for protecting trade secrets and confidential information that has commercial value, including in international industrial espionage contexts, tensions can arise between protection of information disclosed to or gathered by the federal government and the government's obligations of public disclosure under the Freedom of Information Act (FOIA).[6] Notably, Exemption 4 of FOIA recognizes and addresses the need for the government to protect from disclosure under FOIA "trade secret and commercial or financial information obtained from a person and privileged or confidential." Unfortunately, despite the

---

[2] The Order defines "artificial intelligence" or "AI" in accordance with the language of 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. Order, Sec. 3(b). Title 15 includes Chapter 119 – the National Artificial Intelligence Initiative – which places a sweeping set of responsibilities and powers in the President to achieve US leadership in AI research and development, as well as "integration across all sectors of the economy and society."

[3] "Watermarking" is defined in the Order as: "[t]he 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." Order, Section 3(gg).

[4] *See, e.g.,* Order, Sections 4.5(a)(watermarking); 5 .2(d)(theft prevention; enforcement).

[5] As used in the Order, "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." Order Sec. 3 (d).

[6] 5 U.S.C. § 552, *see also*, FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 (2016).

clear intention of Exemption 4, there is also a clear possibility of intentional or unintentional disclosure. Also, courts that engraft an ill-conceived bias in favor of disclosure onto Exemption 4 can wreak havoc on legitimate public, commercial, and national interests.[7]

Some of the above-mentioned dangers can be addressed through proper and properly updated training.[8] There should be a clear and rapidly implemented mandate under the Order, or the recommendations generated under it, that federal officers, employees, agents, and relevant contractors receive regular, intensive and frequently updated training on best practices and U.S. interests in safeguarding trade secret and confidential information, especially in the context of AI.[9] The point is that the Order, or the operations under it, need to create a "loose lips sink ships" ethos for those who may gain access to valuable third party information through the operation and implementation of the Order's directives. Some extra training in, for example, the criminal law that applies to unauthorized disclosures by federal officers, employees and certain agents and contractors – *e.g.,* 18 USC § 1905 – should also be a priority under the Order. (Updating that law and others to provide stricter penalties could also be helpful.) Also, as noted above, it would be beneficial to make the regularly updated training programs mandatory for federal contractors who gain access to trade secret and confidential information. Finally, model training programs could be made available to members of the judiciary, as well as State officials and employees.

In other areas of IP, the Order directs the U.S. Copyright Office to issue recommendations to the President on potential executive actions relating to copyright and AI.[10] Similarly, the Order directs the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office to provide guidance on the application of U.S. patent law to inventions generated in whole or part by AI.[11] In this context, the Order emphasizes that "[p]romoting responsible innovation, competition, and collaboration . . . requires investments in AI-related education, training, research and capacity, while simultaneously tracking novel intellectual property (IP) questions and other problems to protect inventors and creators." [12]

At present, both the Copyright Office and the Patent Office will refuse to apply their respective forms of intellectual property to protect creations made wholly by AI, without any acknowledged human creativity or inventiveness.[13] Although these notions are "in line" with traditional thinking,

---

[7] *See, e.g., New York Times Co. v. U.S. Food and Drug Administration,* 529 F. Supp. 3d 260 (SDNY 2021) for an example of an arguably misdirected approach to Exemption 4.

[8] There are sections in the Order that mandate training, but routine, intensive, and regularly updated training programs, as contemplated in this discussion, are not clearly addressed. *See e.g.,* Order. Sec. 5.2, Sec. 10.2(g). However, there are a number of Sections in the Order that can be interpreted broadly enough to authorize consideration of such training programs. The key is that there needs to be an emphasis on such "introspective" programs and their formulation.

[9] Section 4 of the Order – titled "Ensuring the Safety and Security of AI Technology" – treats the development of best practices and guidelines, but the focus does not include an express directive to emphasize training of federal officers, employees and contractors on measures to avoid (and penalties for) inappropriate disclosures of third party trade secrets and otherwise proprietary confidential information.

[10] Order Sec. 5.2(c) (iii).

[11] Order, Sec. 5.2(c)(i)-(ii).

[12] Order Sec. 2(b).

[13] On February 14, 2022, the Review Board of the United States Copyright Office issued its opinion rejecting applicant Thaler's claim that the creations of his Creativity Machine qualified as copyrightable subject matter. In the Board's

they rely on narrow (perhaps outmoded) ideas on how best to encourage and capitalize on innovation. These notions also raise Constitutional issues of how best to define "authors" and "inventors." Missing from the Order, however, is a clear and sufficiently emphasized directive for the agencies to explore and propose other potential forms of protection for AI generated works and inventions. For example, when the Supreme Court held that the Patent and Copyright Clause of the Constitution does not authorize federal protection of trademarks,[14] Congress simply reverted to its powers under the Commerce Clause of the Constitution – and the federal trademark registration system was born.[15] Therefore, if AI-generated content and inventions cannot be protected under the Patent and Copyright Clause neither Congress nor the States would be precluded from fashioning other protections based on their abilities to control commerce and act against unfair competition. Also, States have stepped in when federal law did not protect sound recordings[16] or individuals' rights to control commercial exploitation of their identifying features (so-called "rights of publicity").[17] Individual States with the highest commercial interests in AI developments might be able to flex their muscles in the areas of AI-generated contents and inventions. For example, in *States Take The Lead on Regulating Artificial Intelligence*, authors Lawrence Norden and Benjamin Lerude point out that "30 states have passed more than 50 laws over the last five years to address AI in some capacity, with attention greatly increasing year over year."[18] Potential state-law based protection for AI generated works (beyond the protections afforded by State trade secret laws) is still open to detailed exploration. Many might see such individual State initiatives as a piecemeal and chaotic approach – potentially subject to preemption by federal law. Others might see such efforts as a welcome impetus to address arcane and outmoded concepts of authorship and invention that can unnecessarily discourage or devalue AI-assisted productivity.

In short, while the Order is quite sweeping and comprehensive, there is room for expansion or clarification of its directives to address a number of critical issues that impact AI-related IP generation, acknowledgement, ownership, and enforcement. Members of industry and academia, as well as legislators and members of the public, will need to step in and be vocal to ensure that

---

words: "[T]he [Copyright] Office is compelled to follow Supreme Court precedent, which makes human authorship an essential element of copyright protection." Board Letter, p. 4, citing *Burrow-Giles Lithographic Co. v. Sarony*, 111 U.S. 53, 56-59 (1884) (photography); *Mazer v. Stein,* 347 U.S. 201, 214 (1954)(sculpture); and *Goldstein v. California,* 412 U.S. 546, 561(1973) (audio recordings). *See also,* Dec. 11, 2023 Copyright Office Review Board opinion, Second Request for Reconsideration for Refusal to Register SURYAST (SR # 1-11016599571; Correspondence ID: 1-5PR2XKJ). A good description of the Patent Office's approach can be found in *Thaler v. Hirshfeld*, 558 F.Supp.3d 238 (E.D. Va. 2021); *aff'd, Thaler v. Vidal*, 43 F.4th 1207 (Fed Cir. 2022), *petition for cert.,* No. 22-919 (March 21, 2023).

[14] *Trademark Cases,* 100 U.S. 82 (1879).

[15] Most of current Federal trademark law, which includes much more than registration, can be found in the Lanham Act, as codified in Title 15 of the U.S. Code.

[16] *See e.g.,* https://ask.loc.gov/recorded-sound/faq/313179 (last accessed Dec. 29, 2023).

[17] *See, e.g., Right of Publicity, https://rightofpublicity.com/ (*last accessed Dec. 29, 2023*); Zacchini v. Scripps-Howard Broadcasting Co.,* 433 U.S. 562 (1977).

[18] Published by the Brennan Center For Justice on Nov. 1, 2023; updated Nov. 6, 2023; https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-artificial-intelligence#:~:text=Some%20states%20%E2%80%94%20California%2C%20Colorado%2C,perpetuate%20bias%20against%20protected%20classes. (last accessed Dec. 29, 2023).

the Order does not result in an incomplete or misdirected approach to IP and its vital role in protecting rights that drive U.S. social, economic, and technological interests. This may require new forms of intellectual property or a practical rethinking of the definitions of "authorship" and "inventorship." Also, the Order is somewhat outward looking when it comes to certain risks – a clear and intensive introspective emphasis on robust training programs for federal officers, agents, employees, and contractors on safeguarding third party information entrusted to them under the federal government's AI programs would be very welcome.