Volume 10, No. 1 | January-February 2027

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Editor's Note: Contrasting Strategies
Victoria Prussen Spears

AI, Intellectual Property, and National Security: Understanding the Administration's Contrasting Strategies
Armin Ghiam and Andre Earls

The Evolving AI Patchwork: Balancing U.S. State Shifts and EU Mandates in Deal Negotiations
David A. Toy, Thomas J. Petrie, and Colin Harris

Adapting Error Resolution to Agentic AI Payments
David A. Stein

AI Is Making Phishing Scams Almost Impossible to Spot—5 Steps Employers Should Take to Combat Latest Threat
Daniel Pepper and Michael Steele

Indian Gaming and Prediction Markets: On a Collision Course?
Blaine I. Green and Allan C. Van Vliet

Prediction Markets Are Creating a New Insider Trading Frontier for Biotech and Pharmaceutical Companies
Chelsea Anderson and Noah Solowiejczyk

CFTC Targets George Santos for Manipulative Trading in State of the Union Event Contract
John C. Murphy, Katherine R. Goldstein, James Joseph Benjamin Jr., Michael A. Asaro, Peter I. Altman, Parvin Daphne Moyne, and Lance Jasper

Different Shoppers, Different Prices: The Federal Trade Commission Takes Aim at Personalized Pricing
Allyson L. Chavez, Anna M. Behrmann, and Kathy L. Osborn

Third Circuit Revives Algorithmic Price-Fixing Suit Against Atlantic City Hotels
Alexis Gilman and Drew Wilson

Model Cloning of a Competitor's AI: Fair Competition or Potential Liability?
Brian W. Nolan, Reginald R. Goeke, Adam S. Hickey, Thea Kendler, and Micheal Antifaoff

Automating the Impact Assessment, and the Limits of AI Compliance
Adilson Fernandes Braga Junior

The UK ICO's New Statutory Duty to Produce an AI Code of Practice: What It Means for Businesses That Use AI
James Castro-Edwards

FULL COURT PRESS
part of Clio

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 10, No. 1 | January–February 2027

7 **Editor's Note: Contrasting Strategies**
Victoria Prussen Spears

11 **AI, Intellectual Property, and National Security: Understanding the Administration's Contrasting Strategies**
Armin Ghiam and Andre Earls

17 **The Evolving AI Patchwork: Balancing U.S. State Shifts and EU Mandates in Deal Negotiations**
David A. Toy, Thomas J. Petrie, and Colin Harris

23 **Adapting Error Resolution to Agentic AI Payments**
David A. Stein

33 **AI Is Making Phishing Scams Almost Impossible to Spot—5 Steps Employers Should Take to Combat Latest Threat**
Daniel Pepper and Michael Steele

37 **Indian Gaming and Prediction Markets: On a Collision Course?**
Blaine I. Green and Allan C. Van Vliet

43 **Prediction Markets Are Creating a New Insider Trading Frontier for Biotech and Pharmaceutical Companies**
Chelsea Anderson and Noah Solowiejczyk

49 **CFTC Targets George Santos for Manipulative Trading in State of the Union Event Contract**
John C. Murphy, Katherine R. Goldstein, James Joseph Benjamin Jr., Michael A. Asaro, Peter I. Altman, Parvin Daphne Moyne, and Lance Jasper

55 **Different Shoppers, Different Prices: The Federal Trade Commission Takes Aim at Personalized Pricing**
Allyson L. Chavez, Anna M. Behrmann, and Kathy L. Osborn

61 **Third Circuit Revives Algorithmic Price-Fixing Suit Against Atlantic City Hotels**
Alexis Gilman and Drew Wilson

67 **Model Cloning of a Competitor's AI: Fair Competition or Potential Liability?**
Brian W. Nolan, Reginald R. Goeke, Adam S. Hickey, Thea Kendler, and Micheal Antifaoff

75 **Automating the Impact Assessment, and the Limits of AI Compliance**
Adilson Fernandes Braga Junior

85 **The UK ICO's New Statutory Duty to Produce an AI Code of Practice: What It Means for Businesses That Use AI**
James Castro-Edwards

EDITOR-IN-CHIEF

Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Jennifer A. Johnson
Partner, Covington & Burling LLP

Paul B. Keller
Partner, Allen & Overy LLP

Garry G. Mathiason
Shareholder, Littler Mendelson P.C.

James A. Sherer
Partner, Baker & Hostetler LLP

Elaine D. Solomon
Partner, Blank Rome LLP

Edward J. Walters
Chief Strategy Officer, vLex

John Frank Weaver
Director, McLane Middleton, Professional Association

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, an imprint of Clio and Themis Solutions, Inc..
Copyright 2027 Full Court Press, an imprint of Clio and Themis Solutions, 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 Full Court Press, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: David Nayer
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Full Court Press)

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.

Copyright © 2027 Full Court Press, an imprint of Clio and Themis Solutions, Inc.

All Rights Reserved.

A Full Court Press, Clio, Publication

https://www.fastcase.com/

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:

David Nayer, Publisher, Full Court Press at david.nayer@clio.com or at 202.999.4777

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)

Model Cloning of a Competitor's AI: Fair Competition or Potential Liability?

Brian W. Nolan, Reginald R. Goeke, Adam S. Hickey, Thea Kendler, and Micheal Antifaoff*

In this article, the authors discuss the debate over the lawfulness of model distillation attacks and discuss governmental actions and legal remedies that may become available to industry participants.

Over the past several months, artificial intelligence (AI) industry participants have debated the propriety and potential remedies for "model distillation attacks," particularly where such actions are initiated by Chinese model developers. Just recently, a number of U.S. government agencies published a joint Cybersecurity Advisory[1] to highlight the scope of these actions, some of the techniques used, and recommending mitigations to reduce their impact.

Some AI executives argue that model distillation attacks represent unlawful conduct that threatens U.S. dominance in AI models, and create asymmetric incentives for investment in AI development. They argue that U.S. model developers should be protected using U.S. trade and sanctions laws or other civil remedies in order to incentivize AI research. Other executives have argued that model distillation is a common industry practice and that it is important to protect the principle that "you can learn from anything you can observe." This debate will play out over the coming years through civil litigation and potential government intervention. The potential governmental actions and legal remedies are addressed below.

Background on Model Distillation Attacks

In machine learning, "distillation" or "model distillation" is a widely used technique for transferring capabilities from a larger, more expensive "teacher" model into a smaller, cheaper "student"

Robotics, Artificial Intelligence & Law / January-February 2027, Vol. 10, No. 1, pp. 67-74
© 2027 Full Court Press. All rights reserved
ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

model. Distillation first involves systematically querying the teacher model and collecting its outputs. Then, using the teacher's outputs, the student model is taught to reproduce the teacher's output across a broad range of inputs. Once trained, much smaller student models can approximate a teacher model's performance at a reduced cost. Model developers frequently use distillation to create mobile, edge, or cost-sensitive versions of their larger model, which are less resource intensive but can deliver similar performance.

Model cloning—sometimes also called a "distillation attack"—uses the same technique to improve a third-party's model. Model cloning involves a third-party systematically querying another company's model—often through an application programming interface (API) or product interface—and then using the model's outputs to train a competing model. The third-party sends large volumes of prompts to the target model, collects the responses, and then uses the prompt-response pairs as training data for its own system. The resulting model can approximate the target model's performance without the third-party having invested in research, data curation, or computational resources.

Both foreign and domestic actors are performing model cloning. To date, a number of Chinese AI companies have been publicly accused of performing model cloning against leading American frontier models, including bypassing terms of service by using thousands of fraudulent accounts. But American companies have also conceded that they performed model distillation against rival AI models to develop their own models, at least in part.

Government Intervention

The U.S. government has increasingly signaled its willingness to intervene when foreign companies perform model cloning against American AI company models. There are a variety of tools the government may draw on, including placing entities on either the Specially Designated Nationals List (SDN) or the Entity List and pursuing criminal prosecution of the entities.

SDN List

Executive Order 13694 empowers the Department of the Treasury to place foreign entities engaged in significant malicious

cyber-enabled activities on the SDN List. Placement on the SDN List (commonly known as becoming sanctioned or designated) results in the entity's assets being frozen and restricts their access to the U.S. financial and business systems, among other things. Placement on the SDN List functionally prevents an entity from doing business in U.S. dollars anywhere in the world.

Entity List

The U.S. government may also put foreign entities or individuals on the Department of Commerce's Entity List, meaning they are prohibited from receiving commodities, software, and technology that are subject to U.S. export controls without a license for export from Commerce. Entity List designation results from a finding that a person is reasonably believed to be involved in activities contrary to U.S. national security or foreign policy interests. Placement on the list could cut off a foreign company accused of model cloning from the advanced chips, cloud computing infrastructure, and development tools it needs to train and deploy its models. In the semiconductor and AI space, the government has added hundreds of entities to the Entity List, many of which are based in China. Short of an Entity Listing (and more quickly), Commerce could limit the specific items that can be exported to particular entities (a process it used to temporarily restrict Anthropic's Mythos and Fable 5 models in June 2026).

EEA Prosecution

The government can also prosecute foreign entities under the Economic Espionage Act (EEA) for criminal misappropriation of trade secrets. The EEA provides two criminal pathways under Title 18. Section 1832 targets anyone who steals or misappropriates a trade secret related to a product or service in interstate or foreign commerce, carrying penalties of up to 10 years' imprisonment for individuals and fines up to the greater of $5 million or three times the value of the stolen secret for organizations. Where the theft is committed with the intent or knowledge that it will benefit a foreign government, instrumentality, or agent, Section 1831 escalates the penalties to 15 years' imprisonment and organizational fines of up to the greater of $10 million or three times the stolen

secret's value. Critically, per Section 1837, these provisions reach conduct occurring outside the United States if the offender is a U.S. person or entity, or if any act in furtherance of the offense was committed within the United States. In practice, however, criminal prosecution of foreign entities faces significant jurisdictional and enforcement headwinds: obtaining personal jurisdiction over offshore actors, securing evidence located abroad, and executing any resulting judgment all present challenges that have recently led to extensive appeals, if not outright dismissal or acquittal, in trade secret prosecutions of foreign companies.

Practical Challenges to Seeking Governmental Help

While U.S. government intervention may be beneficial in addressing model cloning, it is not without risk. The U.S. government will likely expect companies to share non-public information about the nature of the model cloning, how the U.S. model was vulnerable to the cloning, and how the U.S. company was economically damaged. Engaging the government also changes the narrative and may result in less or no control over enforcement decisions, potentially impacting availability of civil remedies.

Civil Legal Remedies

AI companies seeking protection from model cloning may also turn to civil legal remedies to deter and compensate them for distillation attacks. Remedies may include contract claims based on breach of terms-of-service restrictions, state law unfair competition claims, and trade secret misappropriation claims. Such cases require obtaining jurisdiction over foreign actors, proving the legal violation, overcoming defenses, and quantifying any potential damages. Legal claims filed with the U.S. International Trade Commission (ITC) present an additional option if models are embedded in physical products.

Contract Claims

Nearly every major AI platform prohibits the use of model outputs to train competing systems or to reverse engineer system

prompts, data compilations, and other aspects of the model. These terms-of-service restrictions serve a dual purpose: they provide a direct contractual claim against users who violate them, and they bolster trade secret protection by helping establish that the model owner took reasonable steps to maintain secrecy and that any extraction occurred through "improper means." Claims based on terms-of-service violations have recently proliferated in the context of automated scraping of websites and the use of AI agents in accessing merchant sites. Such claims are often combined with claims under the Computer Fraud and Abuse Act. Those cases raise complex issues regarding whether a party accessing the site agreed to the relevant terms, whether the targeted conduct breached the terms of service, and whether the terms of service can limit access to publicly available information. Some courts have found efforts to block copying of uncopyrightable facts as preempted by copyright law.[2] There are also practical challenges to such claims. Where thousands of accounts are generated to distill the model, even identifying the information distilled or the party directing the distillation may pose material hurdles. In addition, those cases require obtaining jurisdiction over the entities performing the distillation. Finally, contractual and statutory damage limits may impact the available relief.

Unfair Competition and Unjust Enrichment

State unfair competition laws and unjust enrichment claims provide additional tools to AI model developers. Under many states' laws, a claim for unfair competition lies where a party injures another by misappropriating an asset in bad faith (New York) or through unfair, unlawful, or fraudulent conduct (California). Content owners have asserted such claims against AI model developers that scraped sites to train their models, including where a party uses the misappropriated fruits to compete with the model developer. Claims of unjust enrichment are also an option, including where enforcement of contractual terms may not be possible. Unjust enrichment and unfair competition claims may enable additional remedies, including recovery of the distiller's profits and injunctive relief.

Trade Secret Misappropriation

Strong terms of service combined with technical controls such as rate limits, anti-automation measures, and account verification could provide access to actions under the Defend Trade Secrets Act (the DTSA) codified at 18 U.S.C. § 1836. Trade secret law covers a wide breadth of information provided that the information derives independent economic value from not being generally known or readily ascertainable, and whose owner has taken reasonable measures to keep it secret. The outputs of a frontier model, to the extent they reflect proprietary training data, architectural choices, and fine-tuning investments, may qualify.

The DTSA creates liability for anyone who obtains such information through "improper means," which includes theft, misrepresentation, breach of a duty to maintain secrecy, and espionage through electronic or other means. Misappropriation, however, does not include reverse engineering or independent derivation through lawful means, and defendants in distillation disputes may assert that querying a publicly available API is simply a form of reverse engineering. Further, defendants might also argue that the AI developer failed to take reasonable steps to protect its trade secrets if the model was available without mechanisms to cut off users engaging in a high volume of calls to the model. This highlights the importance for a company to implement legal (e.g., terms-of-service limitations) and technical controls (e.g., monitoring and controlling model activity) to preserve trade secret misappropriation allegations.

While little judicial precedent analyzes model cloning under the DTSA, courts' assessment of computer data scraping under the DTSA provides some insights. In *Compulife Software, Inc. v. Newman*,[3] the Eleventh Circuit addressed a scenario in which a competitor used automated queries to extract the equivalent of a proprietary database from a publicly accessible website. While fact-specific, the court explained that the use of fake accounts, violation of terms of service, and systematic extraction far exceeding any legitimate use could amount to misappropriation, rather than permissible reverse engineering. In addition to providing injunctive relief, the damages from such claims may extend to extraterritorial activity provided that any "act in furtherance" of the misappropriation occurred in the United States.[4]

ITC Action

While challenges in obtaining jurisdiction over a foreign distillation attacker may limit legal claims in federal courts, AI model developers should consider the ITC if they can show the AI is embedded in a physical product as opposed to the model by itself.[5] This might include products developed using the competing model or products with an embedded version of the competing model. The ITC can issue an exclusion order directing U.S. Customs to block the offending imports from entry—regardless of whether the foreign respondent submits to personal jurisdiction or has U.S. assets. Critically, ITC exclusion orders apply even where the misappropriation occurred entirely outside the United States by a non-U.S. entity.[6] Consider a frontier model that can predict novel protein structures. If a foreign competitor extracts that model's capabilities through model cloning and uses the resulting model to identify and develop a new pharmaceutical compound, the physical drugs entering the U.S. market could be challenged as articles that flow from trade secret misappropriation. The same theory could reach AI-enabled hardware—whether edge devices, autonomous vehicles, robotics systems, or consumer electronics—that incorporate or provide access to a model built using model cloning. As distilled models are used to develop new drugs or become embedded in physical products rather than delivered solely through cloud APIs, the ITC's "articles" requirement becomes easier to satisfy.

Conclusion

As AI models grow more capable and more expensive to develop, companies will need a strategy to protect the proprietary knowledge embedded in those models. While the governmental enforcement and legal frameworks discussed in this article can offer meaningful protection, none was designed specifically with model cloning in mind. The companies best positioned to handle the legal risks flowing from model cloning are those that approach the problem holistically. Companies should consider governmental enforcement tools and how they might help or hinder the company's goals, they should implement rigorous technical safeguards combined with well-crafted contractual protections, and they should have subject matter experts—across at least the subjects mentioned

in this article—who can help them determine which remedies will best meet their goals.

Notes

* The authors, attorneys with Mayer Brown, may be contacted at bnolan@mayerbrown.com, rgoeke@mayerbrown.com, ahickey@mayerbrown.com, tkendler@mayerbrown.com, and mantifaoff@mayerbrown.com, respectively.

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-251a.

2. See, e.g., X Corp v. Bright Data Ltd., 733 F.Supp.3d 832, 850 (N.D. Cal. 2024) (dismissing X Corp's claim against Bright Data for scraping X Corp's site in part because the claim was preempted by the Copyright Act and would extend exclusivity to content that was not copyrightable).

3. Compulife Software, Inc. v. Newman, 959 F.3d 1288 (11th Cir. 2020).

4. Motorola Sols., Inc. v. Hytera Commc'ns Corp. Ltd., 108 F.4th 458 (7th Cir. 2024).

5. ClearCorrect Operating, LLC v. Int'l Trade Comm'n, 810 F.3d 1283, 1299 (Fed. Cir. 2015) ("the literal text … unambiguously expressed intent of Congress is that 'articles' means 'material things' and does not extend to electronically transmitted digital data.").

6. TianRui Grp. Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 1329-1335 (Fed. Cir. 2011).