

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

DOW JONES & COMPANY, INC.
and NYP HOLDINGS, INC.,

Plaintiffs,

v.

PERPLEXITY AI, INC.,

Defendant.

Civil Action No. 1:24-cv-07984-KPF

**STIPULATED SOURCE CODE
PROTOCOL**

Plaintiffs Dow Jones & Company, Inc. and NYP Holdings, Inc. and Defendant Perplexity AI, Inc. (each a “Party,” and collectively, “the Parties”), through their respective counsel of record, hereby submit this Source Code Protocol to protect the confidentiality of certain nonpublic and confidential source code material that will be made available for inspection pursuant to and during the course of discovery for the Court to so order.

Whereas, for good cause shown, IT IS HEREBY ORDERED THAT:

I. General Provisions

1. The Parties acknowledge that this Source Code Protocol is to be read in conjunction with and as a supplement to the Confidentiality and Protective Order entered in this action on August 1, 2025 (Dkt. 62) (“Protective Order”) and the Stipulated Document Production Protocol entered in this action on August 1, 2025 (Dkt. 63). Unless otherwise indicated within this Source Code Protocol, the protections, processes, and limitations set forth in the Protective Order apply to the material that is subject to this Source Code Protocol.

2. In light of these acknowledgements, and based on the representations of the Parties that discovery in this case will involve confidential source code, the public disclosure of which

will cause harm to the producing person and/or third party to whom a duty of confidentiality is owed, and to protect against injury caused by dissemination of confidential source code, this Court finds good cause for issuance of an appropriately tailored confidentiality order regarding source code governing the pretrial phase of this action.

II. Source Code Protocol

3. Any person subject to this Source Code Protocol—including without limitation the Parties to this action, their representatives, agents, experts and consultants, all third parties providing discovery in this action, and all other interested persons with actual or constructive notice of this Source Code Protocol—shall adhere to the following terms.

4. Pursuant to the Protective Order, a Party may designate any information or materials produced by any Party or nonparty as part of discovery in this action as “Highly Confidential – Inspection Data” if the information or material represents confidential, proprietary, or trade secret computer code, computer instructions, or data definitions expressed in a form suitable for input into an assembler, compiler, code interpreter, or other translator, together with associated documentation, such as: comments, revision histories, test scripts and test data, build and configuration files that define or otherwise implement or support the development, training, evaluation, or deployment of software or machine learning models (“Source Code Material”), and disclosure of that material to another Party or nonparty would create a substantial risk of serious harm that could not be avoided by less restrictive means. A document that merely quotes or cites filenames, line numbers, directory names, module names, class names, parameter names, variable names, function names, method names, and/or procedure names (e.g., for notetaking or identification purposes) without reproducing any lines of source code is not Source Code Material but may be designated “Highly Confidential” or “Confidential.” A Party that made and served

the Request for Production of the Source Code Material (“Requesting Party”) may make reasonable requests that if particular documents are made available for inspection that contain both Source Code Material and material that is “Highly Confidential,” “Confidential,” or otherwise non-confidential, that the documents also be produced with the Source Code Material redacted and marked “Highly Confidential” or “Confidential,” if applicable. If the Parties have a dispute regarding such a request, the Requesting Party shall follow the procedures outlined in Paragraph 5 of the Protective Order.

5. For material designated “Highly Confidential – Inspection Data,” the following additional restrictions apply:

a. Source Code Material, to the extent any Party responding to a Request for Production of Source Code Material (“Producing Party”) makes it available for inspection, shall be made available in native format. Access to a Party’s Source Code Material shall be provided only on “standalone” computers (the computer may be interconnected with other devices necessary for accessing the source code (e.g., an external hard drive on which the Producing Party provides the Source Code Material), but may not be linked to any other network, including a local area network (“LAN”), an intranet, or the Internet) (a “Source Code Computer”). Two (2) standalone Source Code Computers shall be made available to the Requesting Party at all times. Should the need reasonably arise, the Requesting Party may request as many as two (2) additional Source Code Computers, approval for which shall not be unreasonably withheld by the Producing Party. Such a request must be made with at least seven (7) days’ prior notice to the Producing Party, which shall respond within five (5) business days. Each standalone Source Code Computer should be connected to two external monitors, an external keyboard, and an external mouse. The hardware specifications of each Source Code Computer will be sufficient for using the source

code review tools utilized in this case. All hardware components of each Source Code Computer and any attached peripherals should be fully functional and in good repair, except for any functionality that is intentionally disabled for security reasons as provided herein. The Requesting Party may request installation of specific software utilities to conduct the source code inspection and analysis in this case on the Source Code Computers, provided that (1) the Requesting Party furnish any necessary software licenses to do so; (2) the Producing Party approves such software tools (which approval may not be unreasonably withheld); and (3) such other software tools are reasonably necessary for the Requesting Party to perform its review of the Source Code consistent with all of the protections herein. To allow the Producing Party reasonable time to prepare the Source Code Computers, the Requesting Party must provide the Producing Party the computer medium (e.g., USB drive, FTP, or web address) containing the requested software utilities and/or required licenses at least ten (10) days in advance of the first inspection in which the software is requested to be on the Source Code Computers. The Producing Party will install and confirm installation of said software on the Source Code Computers as soon as practicable prior to the inspection. Should additional software utilities and/or licenses be deemed necessary by the Requesting Party following the commencement of the inspection, the Parties shall follow the procedure in (1)-(3) above. The Producing Party will install and confirm installation of said software on the Source Code Computers as soon as practicable thereafter. The software will be maintained on the Source Code Computers for the remainder of this litigation or until the Requesting Party notifies the Producing Party in writing that the software is no longer needed.

b. To the extent that the programs or tools used by the Requesting Party record local working files or other records reflecting the work performed by the Requesting Party,

such files and records shall not be reviewed, altered, or deleted by the Producing Party.

c. The Source Code Computers shall be located at the offices of counsel for the Producing Party located at 50 California Street, 22nd Floor, San Francisco, California 94111, or another office of counsel for the Producing Party that is mutually agreed upon by the Producing Party and the Requesting Party. The Parties agree to cooperate in good faith to determine a mutually acceptable location for the Source Code Computers.

d. Any Highly Confidential – Inspection Data information produced in discovery shall be made available for inspection from 9:00 am to 5:00 pm local time (“Normal Business Hours”), provided that the Requesting Party shall provide at least ten (10) days’ notice prior to the first request for access, and at least three (3) days’ notice for each subsequent request. No additional notice is required for access to be made available on consecutive review days, including consecutive review days interrupted by weekends or federal holidays. Source Code Material shall be available for inspection only during Normal Business Hours, Monday through Friday, excluding federal holidays. Requests for access outside Normal Business Hours shall be permitted only upon a showing of reasonable necessity for the efficient prosecution of this case, and the Producing Party may impose a reasonable fee to cover costs of staffing and monitoring outside normal hours. The Parties agree to cooperate in good faith such that maintaining the Producing Party’s Source Code Material shall not unreasonably hinder the Requesting Party’s ability to efficiently and effectively conduct the prosecution or defense of this litigation.

e. The Requesting Party shall provide the name(s) of the individual(s) who will be attending the inspection in writing to the Producing Party at least seven (7) days in advance of the first time that such person inspects the Source Code Computers. All authorized persons inspecting the Source Code Computers shall, on each day they view the Source Code

Computers, sign a log that will include the names of persons who enter the secured room to view the Source Code Computers and when they enter and depart. Proper identification of all authorized persons shall be provided by the Requesting Party prior to any access to the secure inspection room or the secured Source Code Computers. Proper identification requires showing, at a minimum, a photo identification card sanctioned by the government of any State of the United States, by the government of the United States, or by the nation state of the authorized person's current citizenship. Access to the secure inspection room or the secured Source Code Computers may be denied, at the discretion of the Producing Party, to any individual who fails to provide proper identification.

f. The Producing Party shall provide the Requesting Party with information explaining how to start, log on to, and operate the Source Code Computers in order to access the produced Source Code Material on the Source Code Computers. Unless otherwise permitted by this Protocol, the Requesting Party's personnel are prohibited from bringing the following into the secure room: (i) cellular phones, smartphones, or any wireless communication devices; (ii) personal computers, laptops, tablets, or portable computing devices; (iii) recording devices of any kind, including audio recorders, video cameras, or digital recorders; (iv) storage devices, including flash drives, memory sticks, external hard drives, or USB devices; (v) cameras, including digital or film cameras; (vi) wearable electronic devices which allow for the recording or uploading of files; (vii) virtual or augmented reality headsets; (viii) personal digital assistants (PDAs) or similar devices; and (ix) any other electronic devices not explicitly approved in writing by the Producing Party in advance (such approval not to be unreasonably withheld). The only exceptions are medical devices, implants, or equipment reasonably necessary for legitimate medical reasons, and air gapped computers for the purpose of taking such notes ("Air Gapped

Computers”).

g. The Requesting Party shall be entitled to take notes (electronic and non-electronic) relating to the Source Code Materials but may not copy the Source Code Materials into such notes. The Requesting Party shall be entitled to use Air Gapped Computers in the room with the Source Code Computers to take notes. Such Air Gapped Computers shall be supplied by the Requesting Party, fully isolated from networks, with Bluetooth and wireless features disabled. Physical ports on the Air Gapped Computers must be locked or monitored, and cameras must be covered. The Producing Party may inspect the Air Gapped Computers prior to them entering the secure room by requiring the Requesting Party reviewer to demonstrate that the Air Gapped Computers meet the requirements of this provision. Approval of the Air Gapped Computers shall not be unreasonably withheld. Should the Producing Party determine that the Air Gapped Computers do not meet the requirements of this provision, they will in good faith assist the Requesting Party in bringing the computers into compliance. Such inspection shall not unreasonably delay the entrance to the room and shall not in any case involve the Producing Party viewing any file or technology on the Air Gapped Computers not necessary to ensure compliance. Any notes taken under this paragraph shall not include copies or reproductions of portions of the Source Code Material; however, the notes may contain filenames, directory names, module names, class names, parameter names, variable names, function names, method names, procedure names, and other similar identifiers as well as descriptions of their functionality as inferred by the code reviewer. No copies of any portion of the Source Code Material may leave the room in which the Source Code Material is inspected except as otherwise provided herein. The Producing Party shall not review the substance of the notes at any time.

h. Access to material designated “Highly Confidential – Inspection Data”

shall be limited to counsel and up to six (6) outside consultants or experts (i.e., not existing employees or affiliate(s) of a Party) retained for the purpose of this litigation and approved to access such protected materials pursuant to paragraph 6(e) of the Protective Order. For the purposes of this Order, an outside consultant or expert is defined to include the outside consultant's or expert's support personnel within his or her firm, such that the disclosure to a consultant or expert who works with others under his or her direction shall count as a disclosure to a single consultant or expert, provided that each outside person has signed the Certification Regarding Confidentiality and been disclosed under the terms of the Protective Order. Access to and review of the Source Code Material shall be strictly for the purpose of investigating the claims and defenses at issue in the above-captioned case. No person shall review or analyze any Source Code Material for purposes unrelated to this case, nor may any person use any source code gained as a result of reviewing Source Code Material in this case in any other pending or future dispute, proceeding, or litigation.

i. Counsel for the Producing Party may visually monitor the activities of the Requesting Party's representatives during any Source Code Review, but only to ensure that there is no unauthorized recording, copying, or transmission of the Source Code. Such monitoring must take place in a separate room from the Requesting Party's representatives, such as outside the walls of a glass conference room. Under no circumstances shall counsel for the Producing Party be permitted to hear or monitor the conversations of, or review the notes of, the Requesting Party's representatives.

j. A Requesting Party may include protected material designated "Highly Confidential – Inspection Data" in a pleading, exhibit, expert report, discovery document, or other Court document ("Source Code Document"), provided that the Source Code Documents

are also designated “Highly Confidential – Inspection Data,” restricted to those who are entitled to have access to them as specified herein, and, if filed with the Court, filed under seal in accordance with the Court’s rules, procedures, and orders and the Protective Order in this case. The Requesting Party shall only include such excerpts or portions of such Source Code Material as reasonably necessary for the purposes for which such Source Code Material is used. To the extent Source Code Material designated “Highly Confidential – Inspection Data” is quoted or attached as exhibit(s) in a Source Code Document, either (1) the entire Source Code Document will be stamped and treated as “Highly Confidential – Inspection Data,” or (2) those pages containing quoted protected material designated “Highly Confidential – Inspection Data” will be separately stamped and treated as “Highly Confidential – Inspection Data”;

k. No electronic copies of printouts of Source Code Material (as described in paragraph 5(l)) shall be made without prior written consent of the Producing Party, except as necessary to create documents which, pursuant to the Court’s rules, procedures, and order, must be filed or served electronically. The Requesting Party shall only include such excerpts as are reasonably necessary for the purposes for which such part of the Source Code Material is used.

l. The Requesting Party shall be permitted to request a reasonable number of printouts of Source Code Material (which shall presumptively be a total of five hundred (500) pages of Source Code Material for each version of the Source Code Material, per Producing Party), but no more than 25 pages of consecutive source code¹, that is reasonably necessary for the preparation of court filings, expert reports, or other papers, or for deposition or trial, but shall not request paper copies for the purpose of avoiding electronic review on the Source Code Computers in the first instance, all of which shall be designated and clearly labeled “Highly

¹ Source code printout limits apply only to computer code and associated comments.

Confidential – Inspection Data.” The Requesting Party shall maintain a log of all such files that are printed and of any individual who has inspected any portion of the Source Code Material in electronic or paper form. All requested printouts shall be given to the Producing Party for inspection by printing the files requested into PDF format, placing the PDF-printed files in a folder designated for such printouts on the Source Code Computers, and notifying the Producing Party of the request to print the files by identifying them by file path, file name, and line numbers, together with the order in which the files are requested to be printed. Within five (5) business days of such request, the Producing Party shall provide five (5) bates-stamped paper copies of such unobjected pages to the Requesting Party. For use at depositions only, the Requesting Party may request that the Producing Party print three (3) additional paper copies of Source Code Material printouts. The Requesting Party must make its request at least three (3) days before the deposition will occur. These additional copies of Source Code Material shall be collected by the Producing Party at the conclusion of the deposition and destroyed immediately thereafter. The Parties understand and agree that the above page limitations were agreed upon without knowledge of the number of pages of source code that may or should be necessary for use in this Action and therefore agree to meet and confer in good faith in the event a Party requests a reasonable enlargement. Such printouts will be printed on plain white copier paper, in the format requested by the Requesting Party, with appropriate confidentiality designations on the face thereof.

m. The Producing Party may challenge the amount of requested Source Code Material printouts pursuant to the dispute resolution procedure and timeframes set out in paragraph 5 of the Protective Order.

n. Any printed pages of Source Code Material, and any other documents or

things reflecting Source Code Material that have been designated as “Highly Confidential – Inspection Data” may not be copied, digitally imaged, or otherwise duplicated, except in limited excerpts as outlined in paragraph 5(j).

o. Should such printouts be transferred back to electronic media, such media shall be labeled “Highly Confidential – Inspection Data” and shall continue to be treated as such.

p. If the Requesting Party’s outside counsel, consultants, or experts obtain printouts of Source Code Material, the Requesting Party shall ensure that such outside counsel, consultants, or experts keep the printouts in a secured locked area in the offices of such outside counsel, consultants, or expert. The Requesting Party may also temporarily keep the printouts at: (i) the Court for any proceeding(s) relating to the Source Code Material, for the dates associated with the proceeding(s); (ii) the sites where any deposition(s) relating to the Source Code Material are taken, for the dates associated with the deposition(s); and (iii) any intermediate location reasonably necessary to transport (e.g., a hotel prior to a Court proceeding or deposition), provided that the printouts are kept in a secure manner that ensures access is limited to the persons authorized under this Order.

q. Material designated “Highly Confidential – Inspection Data” may only be transported by the Requesting Party at the direction of a person authorized under paragraph 5(h) above to another person authorized under paragraph 5(h) above, on paper via hand carry, or by Federal Express or other similarly reliable courier. Printouts of Source Code Material may only be transported for the purpose of Court proceeding(s) or deposition(s) as set forth in paragraph 5(p) above and is at all times subject to the transport and labeling restrictions set forth herein. The Source Code Materials may not be scanned into a computer. However, portions of Source Code Materials may be manually typed into a computer or captured as photographic images and

uploaded to a computer. For purposes of Court filings and proceedings, citations to line numbers and photographic images or embeddings of Source Code Materials may be used consistent with paragraph 14 of the Protective Order.

r. All copies of any material designated “Highly Confidential – Inspection Data” in whatever form shall be securely destroyed if they are no longer reasonably necessary in this Action (e.g., extra copies at the conclusion of deposition). Copies of material designated “Highly Confidential – Inspection Data” that are marked as deposition exhibits shall not be provided to the court reporter or attached to deposition transcripts; rather, the deposition record will identify the exhibit by its production number(s). Following conclusion of this Action and expiration of all appeal periods, all copies of Source Code Material designated “Highly Confidential – Inspection Data,” including all printouts, handwritten notes, USB devices, and any documents derived from or referencing the Source Code Material, shall be securely destroyed within fifteen (15) days. “Securely destroyed” means shredded, burned, or permanently deleted (for electronic media). For the avoidance of doubt, where reasonably possible, Source Code Material will be excluded from any automatic backups. If Source Code Material is inadvertently or reasonably unavoidably included in an automatic backup, this does not require the purging of such copies from automatic backups of devices; however, should such backups be restored or otherwise discovered, the reviewer shall promptly and securely destroy any Source Code Material upon discovery of such material. The Requesting Party shall provide written certification, provided by each expert and outside counsel with access to Source Code Material, stating: (i) that all such materials have been destroyed; (ii) the method of destruction; (iii) the date of destruction; (iv) that no copies remain in any form whatsoever except in automatic backups as stated in this paragraph, and (v) that they shall not use any knowledge

gained from review of the Source Code Material in any future work or endeavor.

s. Nothing in this Source Code Protocol shall alter or change in any way the requirements of the Protective Order. In the event of any conflict, however, this Source Code Protocol shall control for any Source Code Material made available for inspection.

6. For the avoidance of doubt, nothing in this Source Code Protocol shall preclude the Parties from negotiating specific protocols for review of any specific Source Code Materials or other material designated Confidential or Highly Confidential.

AGREED:

By: /s/ Justin M. Romeo

William P. Barr (*pro hac vice*)
Paul T. Cappuccio (4092508)
Counsel of Record
Justin M. Romeo (*pro hac vice*)
Genevieve M. Kelly (*pro hac vice*)
TORRIDON LAW PLLC
801 Seventeenth Street NW, Suite 1100
Washington, DC 20006
Telephone: (202) 249-6900
pcappuccio@torridonlaw.com
jromeo@torridonlaw.com
gkelly@torridonlaw.com

Brett D. Katz (BK6685)
TORRIDON LAW PLLC
800 Westchester Avenue, Suite N-641
Rye Brook, NY 10573
Telephone: (646) 787-9290
bkatz@torridonlaw.com

Susan J. Kohlmann
Alison I. Stein
Gianni P. Servodidio
JENNER & BLOCK LLP
1155 Avenue of the Americas
New York, NY 10036
Telephone: (212) 891-1600
skohlmann@jenner.com
astein@jenner.com
gservodidio@jenner.com

*Counsel for Plaintiffs Dow Jones & Company, Inc.
and NYP Holdings, Inc.*

Dated: January 16, 2026
New York, New York

By: /s/ Andrew H. Schapiro

Andrew H. Schapiro
William F. Patry
Jessica A. Rose
Dylan I. Scher
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
295 Fifth Avenue
New York, NY 10016
Telephone: (212) 849-7064
andrewschapiro@quinnemanuel.com
williampatry@quinnemanuel.com
jessicarose@quinnemanuel.com
dylanscher@quinnemanuel.com

John B. Quinn
Moon Hee Lee (*pro hac vice*)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
865 S. Figueroa St, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
johnquinn@quinnemanuel.com
moonheelee@quinnemanuel.com

Counsel for Defendant Perplexity AI, Inc.

SO ORDERED



Katherine Polk Failla
United States District Judge

This confidentiality agreement does not bind the Court or any of its personnel. The Court can modify this stipulation at any time. The Court will retain jurisdiction over the terms and conditions of this agreement only for the pendency of this litigation. Any party wishing to make redacted or sealed submissions shall comply with Rule 9 of this Court's Individual Rules of Civil Procedure.