

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF NEW
YORK

**Multi-State Partnership for Prevention, LLC v. Samuel Kennedy,
Kennedy Technology MK, and Kennedy Technology, LLC**

No. 24-CV-00013 (JMW) (E.D.N.Y. Feb. 11, 2026) · No. 24-CV-00013 (JMW) · Decided February 11, 2026

OPINION

Multi-State Partnership for Prevention, LLC v. Samuel Kennedy, Kennedy Technology MK, and
Kennedy Technology, LLC

PER CURIAM.

UNITED STATES DISTRICT COURT CLERK

EASTERN DISTRICT OF NEW YORK 2/11/2026

-----X

U.S. DISTRICT COURT

MULTI-STATE PARTNERSHIP FOR

EASTERN DISTRICT OF NEW YORK

PREVENTION, LLC,

LONG ISLAND OFFICE

Plaintiff,

ORDER

-against-

24-CV-00013 (JMW)

SAMUEL KENNEDY, KENNEDY

TECHNOLOGY MK, and KENNEDY

TECHNOLOGY, LLC,

Defendants. -----X A P P E A R A N C E S: Jordan

Fletcher Fletcher Law, PLLC 234 Fifth Avenue, 2nd Floor New York, NY 10001 Attorney for

Plaintiff Kathleen Rose Fitzpatrick KRF Legal 249 Smith St, #118 Brooklyn, NY 11231 -and-

Peter Brown Peter Brown & Associates PLLC 260 Madison Avenue, 16th Floor New York, NY

10016 Attorneys for Defendants WICKS, Magistrate Judge: This latest discovery motion raises

the question of not whether source code should be produced, but how? Plaintiff Multi-State

Partnership for Prevention, LLC (“Plaintiff” or “MSPP”) commenced this declaratory judgment

action against Defendants Samuel Kennedy (“Kennedy”) and Kennedy Technology MK

(collectively, the “Defendants”) alleging inter alia non- infringement of copyright, arising out of

Plaintiff’s development of a computer software program, PrepMod, developed in the early stages

of the COVID-19 pandemic. (See generally, ECF No. 22.) As the parties are proceeding with fact

discovery, although there is no dispute that source code should be produced, the issue presented is how it should be produced. (See ECF Nos. 93, 103-04.) The PrepMod software is what Plaintiff had originally contracted with Defendant to service. (See ECF Nos. 98-1 at 5.) The software was “an end-to-end vaccine administration and tracking solution which automated key aspects of mass vaccination delivery in clinical and non- clinical setting.” (Id. at ¶ 2.) The software updates, which Kennedy claims to own, is known as PrepMod. (ECF No. 103-2 at 1-2.) In sum, the parties dispute the way in which Plaintiff should produce the PrepMod to Defendants. A dispute that has been on-going since April of 2024. (See ECF No. 93 at 1, 3.) At first, Plaintiff took issue with Kennedy’s ability to review the source code and previously asked this Court to designate the source code as “Attorneys’ Eyes Only”. (See ECF Nos. 67, 93, 104.) That application was denied. (See ECF No. 70.) Now, Plaintiff attempts to compromise and place further restrictions if Kennedy is provided with the production. (See ECF No. 104.) Defendants propose that the production of PrepMod should be produced using the GitHub platform because the PrepMod is already on that platform (“Defendants’ Option”). (ECF No. 103 at 1.) Plaintiff offers three alternatives: (i) an in-person review on a secure, air-gapped machine, in a manner similar to that described in the District of Delaware’s protocol (“Plaintiff’s First Option”), (ii) a remote review used by logging into a secure virtual environment during certain hours while monitored (“Plaintiff’s Second Option”), and (iii) another remote review with enhanced biometric security tools, such as facial recognition and mobile phone detection (“Plaintiff’s Third Option”). (ECF No. 104 at 4-5.) A hearing was held on January 27, 2026, where the Court heard the parties’ respective arguments on the issue. (See Electronic Order dated 1/27/2026.) Following the hearing, the parties were afforded opportunity to submit supplemental filings, and additional letter briefs were filed. (ECF Nos. 109, 111.) For the reasons set forth below, Defendants’ Option subject to this Court’s further rulings described herein is approved and Defendants’ Motion (ECF No. 103) is GRANTED.

DISCUSSION

Defendants seek the Court’s ruling on production of the PrepMod source code as the parties are now at an impasse. Plaintiff disagrees with that assertion. Plaintiff argues that the meet-and-confers were shortened and thus, this motion is really premature. (ECF No. 104 at 3.) Nonetheless, the Court continues to address the instant motion. Additionally, in Defendants’ motion, there is mention of another case brought by Plaintiffs for, inter alia, misappropriation of trade secrets against a party unrelated to this matter. (ECF No. 103 at 3 n.3.) That case is Multi- State Partnership for Prevention, LLC v. Deloitte Consulting, LLP et al, Case No. 1:24-cv-09013 (PKC), and is currently awaiting decision on a motion to dismiss. Defendants point in bringing this to the Court’s attention is that Plaintiff never treated the PrepMod source code as a trade secret here and should not be subject to such additional protection. (ECF No. 103 at 3.) Plaintiff at the hearing, disagreed and stated it is “default” to treat source codes as trade secrets. (ECF No. 108 at 25-26.) Importantly, that issue is not before the Court currently, and as such, the analysis set

forth below is not changed due to the unrelated matter. Defendants argue that using the GitHub platform is the best solution. (ECF No. 103 at 1.) GitHub is the platform that Defendants used to develop the code and Defendants allege that Plaintiff used this platform as well for additional developments. (Id.) Defendant Kennedy states that the GitHub platform, is the gold standard source code repository for the development of software products, and it is well-known in the software industry as being secure. GitHub is based on the free software product call Git which is a “version control system.” GitHub provides a platform where which allows a restricted number of users, each using the Git software, to code, modify and comment upon computer software in development. ... GitHub platform is analogous to website “DropBox” in providing a secure location to develop and store software. Every activity on GitHub is monitored and recorded. This repository of activity is invaluable to an experienced programmer in tracking the evolution and functions of a software product. Reviewing the PrepMod source code on GitHub is ideal because it will track all my actions, including downloads. Using the GitHub platform will also keep MSPP’s source code on the servers controlled by Microsoft inside the United States. Review on the GitHub platform is also critical because it contains the “git repository” for all work done on PrepMod. A “git repository” is a digital archive of the history of a body of source code. ... The git repository stores these changes along with identifying the user making the change and the date and time the change was made. Put differently, the git repository details the entire history, development, timeline, evolution, authorship, provenance, and other details of the PrepMod source code, allowing me to see the evolution, if any, of the code from the copy I currently possess ... to the code as it exists today. (ECF No. 103-2 at 2-3.) Defendants further contend that there is no other viable alternative, and GitHub is safe and cost-effective. (ECF No. 103 at 2-3.) Indeed, this Court previously ruled that it is “likewise unpersuaded that Kennedy's presence in Macedonia alone poses any risk to Plaintiff that cannot otherwise be cured through the use of the GitHub platform, which was already used to develop the software at issue in Macedonia.” Multi-State P'ship for Prevention, LLC v. Kennedy, No. 24- CV-00013 (JMW), 2024 WL 5146067, at *5 (E.D.N.Y. Dec. 17, 2024). However, Plaintiff argues that allowing Kennedy to use GitHub as a way to review the source code is not a protective measure as nothing could prevent Kennedy from downloading, modifying, or copying materials. (ECF No. 104 at 4.) Plaintiff also notes that there have been significant modifications to the software since Defendants last viewed it when working together and such a valuable trade secret should not be produced without additional safeguards. (Id.) So, Plaintiff offers the following three alternatives listed: (i) In-person review on a secure, air-gapped machine, in a manner similar to that described in the District of Delaware’s protocol1. This review could occur in New York City, or at one of MSPP’s third-party vendor’s European locations, including in Germany, Austria, or Italy. On information and belief, Kennedy maintains a residence in or is often in New York. (ii) Remote review by logging into a virtual, dedicated and secure environment (e.g., similar to the Citrix platform). Kennedy would only review during pre-defined hours and he would be required to keep his webcam turned on while he reviews so that

MSPP can verify that he is alone in his review (i.e., that he is not exposing the code in-person to another individual) and not photographing or recording the screen with a mobile phone or other device. (iii) Remote review similar to Option 2, but with enhanced biometric security tools, including facial recognition and mobile phone detection, which eliminate the need for Kennedy to review during pre-scheduled hours or to leave his webcam on. (Id. at 4-5.)² All three options according to Plaintiff are similar to GitHub but also protect against any possible downloading functions. (Id. at 5.) Indeed, Plaintiff “is willing to cover the vendor cost, at least for now.” (Id.) Thus, any argument as to cost is moot currently. Early last year, the Court so-ordered the parties’ protective order. (See ECF No. 72.) Within that order, the parties agreed that confidential information shall be utilized by the receiving party and its counsel for this action and “for no other purposes, including any business or competitive purpose.” (See id. at ¶ 7.) Here, Plaintiff fails to explain why the safeguards¹ Defendants attached the protocol to their motion. (See ECF No. 103-3.) The Delaware protocol discusses among other things the use of a protected stand-alone computer, which Defendants argue is not viable because it would restrict Kennedy’s ability to meaningfully review the discovery. (ECF No. 103 at 2-3.)² However, Plaintiff maintains that Defendant Kennedy should not have access to the code because he is not an expert in this case and there is a risk of copying or downloading the code. (Id.) Yet Plaintiffs offer the three alternatives in order to compromise. (Id.) outlined in that order are not sufficient if the GitHub platform is used. Indeed, at the hearing, it was revealed that GitHub has “read-only” options that could alleviate concerns raised by Plaintiff. (See ECF No. 108 at 5-6.) See *Uni-Sys., LLC v. United States Tennis Ass’n, Inc.*, No. 17- CV-147 (KAM)(CLP), 2018 WL 6179433, at *5 (E.D.N.Y. Nov. 27, 2018) (“Accordingly, since Morgan has failed to adequately explain why standard precautions to maintain the confidentiality of the Source Code, such as the ones in place in connection with the hard copy production, are not enough, and since the request to monitor every action by plaintiff’s counsel or their experts is in clear conflict with the plaintiff’s right to work product protection.”); see also *Apple Inc. v. Samsung Elecs. Co.*, No. 11-CV-01846 (LHK), 2012 WL 10817203, at *7-8 (N.D. Cal. Jan. 30, 2012) (granting a protective order for source codes that require maintaining the source code in a safe locked space and only allowing attorneys’ eyes only including outside counsel). Plaintiff continues to take issue with using the GitHub platform and seeks to use an option to produce the source code that prevents any sort of copying. The options appear restrictive and burdensome if as Kennedy asserts, the source code is already on the GitHub platform. (See ECF Nos. 103 at 1; 103-2 at ¶ 6.) If that is the case, then any further expenses to use a different method or a possible third-party vendor, would be at odds with Fed. R. Civ. P. 1, which requires cases to be “just, speedy and inexpensive.” See Fed. R. Civ. P. 1 (“These rules govern the procedure in all civil actions and proceedings in the United States district courts.... They should be construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding.”) Notably, all three options either involve travel, restrict a real review or time restrictions. (ECF No. 111 at 8.)

Plaintiff at the hearing took issue with the possibility of screenshotting. (ECF No. 108 at 6.) Kennedy avers that he must copy or download the source code from GitHub in order to assist his attorneys in the litigation. (ECF No. 108 at 11.) However, he understands he is bound by the confidentiality order issued by the Court. Specifically, Kennedy states “I understand that I must comply with that order, which means I must keep all designated materials— including the PrepMod source code and git history—confidential.” (ECF No. 111 at 3.) This key aspect was emphasized several times at the hearing by the Court, and Plaintiff conceded to this fact several times. (See e.g., ECF No. 108 at 11, 18, 24-25.) “It is now well settled that the literal elements of computer programs, i.e., their source and object codes, are the subject of copyright protection.” *Computer Assocs. Int’l, Inc. v. Altai, Inc.*, 982 F.2d 693, 702 (2d Cir. 1992). Computer languages have been written to facilitate program writing and reading. A program in such a computer language—BASIC, C, and Java are examples—is said to be written in “source code.” Source code has the benefit of being much easier to read (by people) than object code, but as a general matter, it must be translated back to object code before it can be read by a computer. ... Since computer languages range in complexity, object code can be placed on one end of a spectrum, and different kinds of source code can be arrayed across the spectrum according to the ease with which they are read and understood by humans. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 439 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 483 (6th Cir. 2000) (same). A source code is best known as sets of written computer instructions that experts in that field understand. See e.g., *Equistar Chemicals L.P. v. Indeck Power Equip. Co.*, No. 18-CV-4349 (ASH), 2020 WL 4746469, at *2–3 (S.D. Tex. Aug. 17, 2020) (“Software is an interface program that translates the computer coding to an understandable format for the operators and other engineers working with the boilers. This program is commonly referred to as the sourcecode”); *McEnroe v. Mantissa Corp.*, No. 14-CV-12320 (LTS), 2016 WL 7799636, at

*9 n.6 (D. Mass. Feb. 29, 2016) (“the source code, at issue here, is a literal element of a computer program, while the program's sequence, structure, organization and user interface encompass its nonliteral elements”); *ILOG, Inc. v. Bell Logic, LLC*, 181 F. Supp. 2d 3, 7 n.2 (D. Mass. 2002) (“Source code is the series of commands in a specific programming language that direct a computer to perform specific tasks (what is generally thought of as the program), object code is the binary language conversion of the source code (the machine readable code)”). While the Court is sensitive to the need to protect trade secrets that might be contained in a source code, production of source codes is clearly relevant where the subject of the dispute centers around the source code itself. See *Xinuos, Inc. v. IBM Corp.*, No. 22-CV-09777 (CS) (VR), 2024 WL 5010717, at *3 (S.D.N.Y. Nov. 13, 2024) (“Of course, production of source code may be commonplace in patent or copyright litigation, where parties routinely produce code under extremely controlled conditions and undergo the requisite burden in doing so.”) “Where circumstances warrant, a court may imposed restrictions on how the code is actually produced to the requesting party.” Robert A. Matthews, Jr., *Production of computer code—Imposing*

Restrictions on How Source Code is Produced or Reviewed, 7 ANNOTATED PATENT DIGEST § 41:63.60 (Dec. 2025 update). However, “a responding party, not the court or requesting party, is generally best situated to determine and implement appropriate procedures, methodologies, and technologies. ... This has become even more clear in the years since the original publication of The Sedona Principles.” THE SEDONA CONFERENCE, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* A Project of the Sedona Conference Working Group on Electronic Document Retention and Produ, 19 Sedona Conf. J. 1, 120 (2018); see also *In re OpenAI, Inc., Copyright Infringement Litig.*, No. 25-MD-3143 (SHS) (OTW), 2025 WL 3471561, at *4 (S.D.N.Y. Dec. 3, 2025) (quoting *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 120 (2018) (“The Sedona Conference also recognizes that, typically, a ‘responding party ... is generally best situated to determine and implement appropriate procedures, methodologies, and technologies,’ for responding to discovery requests.”)); *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 650 (D. Kan. 2005) (discussing that courts reference the Sedona Conference for guidance on discovery production issues); *Sound Around, Inc. v. Friedman*, No. 24-CV-1986 (DLC) (KHP), 2025 WL 2855353, at *4 (S.D.N.Y. Oct. 8, 2025) (same).

It is beyond peradventure “that source code requires additional protections to prevent improper disclosure because it is often a company's most sensitive and most valuable property.” *Drone Techs., Inc. v. Parrot S.A.*, 838 F.3d 1283, 1300 n.13 (Fed. Cir. 2016). “Source codes are the most sensitive and confidential property [and] ... extreme measures are ordered to protect their confidentiality.” *Via Vadis Controlling GmbH v. Skype, Inc.*, No. 12-MC-193 (RGA), 2013 WL 646236, at *3 (D. Del. Feb. 21, 2013). “There will always be a need to balance convenience and function with security. Too much security can impede the ability of attorneys and [third party service providers] to do their jobs, while too-little security risks exposing sensitive information belonging to the [legal service providers], its clients, or third parties.” *The Sedona Conference Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*, 17 SEDONA CONF. J. 1, 36 (2016). To that same end, the type of inspection of electronic systems must be reasonable. See THE SEDONA CONFERENCE, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* A Project of the Sedona Conference Working Group on Electronic Document Retention and Produ, 19 SEDONA CONF. J. 1, 129 (2018) (“[t]o justify the onsite inspection of a responding party's computer systems, a requesting party must demonstrate that there is a substantial need to discover information about the computer system and programs used (as opposed to the data stored on that system) and that there is no reasonable alternative to an onsite inspection.”) Keeping these principles in mind, it appears that Defendant’s Option is the best protected and efficient way to move forward with production. Since Kennedy is currently North Macedonia and likely does not have the ability to review the source

code in New York in counsel's office, or any other location offered by Plaintiff (see ECF No. 109-1 at 6), GitHub with restrictions is the most practicable way to move forward. "Because source code is guarded so closely, the producing party typically provides it for inspection rather than producing copies of the source code." See Kim Leffert, Graham Buccigross, *Discovery of Source Code—Fashioning a Protective Order*, MAYER BROWN LLP (last visited Jan. 21, 2026), <https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2015/12/electronic-discovery--information-governance--tip/files/151230-chi-edig-tom/fileattachment/151230-chi-edig-tom.pdf> (also noting that inspections typically occur at the offices of the producing party's litigation counsel); see also Alec M. Royka, Matthew M. Zuziak, *Managing source code discovery in patent and high-tech intellectual property litigation*, NIXON PEABODY LLP (Mar. 7, 2025), <https://www.nixonpeabody.com/insights/alerts/2025/03/07/managing-source-code-discovery-in-patent-and-high-tech-intellectual-property-litigation> ("Litigants should consider the location and access to source code when selecting the proper venue for a patent dispute or high-tech intellectual property dispute.") Plaintiff's concerns about copying or downloading the source code are not uncommon. The supplemental brief by Plaintiff continues to address these concerns. (ECF No. 109.) The Court remains unpersuaded as noted at the hearing that the GitHub platform is not the most efficient way to proceed. While Plaintiff's three options add further security measures, Kennedy contends that all can be "easily bypassed or evaded", which would defeat the purpose of Plaintiff's proposals. (ECF No. 111 at 4.) Due to the overall dispute here – ownership of the PrepMod source code – Kennedy must be given access to the source code for review. Kennedy is under an obligation to keep the discovery confidential and is on notice that any unlawful use of the materials provided will result in a breach of the confidentiality order. Separately, it is known practice that unless court ordered or through stipulation, production is provided "as they are kept in the usual course of business or ... a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms." Fed. R. Civ. P. 34(b)(2)(E). See also *Aguilar v. Immigr. & Customs Enf't Div. of U.S. Dep't of Homeland Sec.*, 255 F.R.D. 350, 356 (S.D.N.Y. 2008) (internal citations omitted) (emphasis in original) ("production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, ... where appropriate or necessary in light of the nature of the information and the needs of the case"). With that, there is no dispute that GitHub was the original platform used to develop the PrepMod source code. (See ECF No. 108 at 7, 18.) Neither party, has provided the Court with authority that GitHub has been rejected by courts in these circumstances. Given the above, GitHub will be the platform used for production. However, unfettered access will not be allowed. Plaintiff shall provide "read-only" access and monitor Defendants' actions on GitHub by using the platform's history tools to ensure no modifications have taken place. Any issues or concerns must be raised with the Court immediately. Accordingly, Defendant's Option is the most efficient way to produce the PrepMod

source code at issue.

CONCLUSION

Defendants' Motion (ECF No. 103) is GRANTED, and the PrepMod source code shall be produced on the GitHub platform using the "read-only" feature. Plaintiff is directed to produce the source code on or before March 4, 2026.³ The parties are reminded to file a joint Status Report on or before March 28, 2026, advising the Court of the status of discovery and a proposed discovery schedule for the remaining deadlines. All current discovery dates and deadlines remain in abeyance pending the filing of the joint Status Report. Dated: Central Islip, New York. February 11, 2026 S O O R D E R E D: James M. Wicks /S/

JAMES M. WICKS

United States Magistrate Judge 3 Plaintiff's request to have at least twenty-one days to produce the source code is granted. (ECF No. 109 at 3.)