No.

IN THE

Supreme Court of the United States

IN RE MICRON TECHNOLOGY, INC., MICRON CONSUMER PRODUCTS GROUP, LLC.

ON PETITION FOR A WRIT OF MANDAMUS TO THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

PETITION FOR A WRIT OF MANDAMUS

Kamilyn Y. Choi
Brenna Ferris Neustater
ORRICK, HERRINGTON & SUTCLIFFE LLP
2100 Pennsylvania Avenue, NW
Washington, DC 20037

Jared Bobrow
Jeremy Jason Lang
Diana M. Rutowski
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025

Elizabeth R. Moulton
Counsel of Record
ORRICK, HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105
(415) 773-5700
emoulton@orrick.com

Counsel for Petitioners

QUESTION PRESENTED

When parties enter into the civil-discovery process with an agreed-upon, court-endorsed set of guardrails in a protective order, they reasonably expect those rules to be followed and enforced. That did not happen here. The plaintiff below, a Chinese state-owned entity, sought unsecure paper copies of sensitive technical information about Petitioners' semiconductor chips. The discovery rules governing that request required the plaintiff to show that the paper copies were reasonably necessary to the litigation and not excessive. When Petitioners sought to enforce that rule, the district court abandoned the terms of the parties' agreement and rubber-stamped plaintiff's request.

In doing so, the court ignored the parties' agreed-to limits on production of paper copies, the readily available alternative means for securely producing the same information, and the Executive Branch's designation of that Chinese state-owned entity as posing "a significant risk of becoming involved in activities contrary to the national security or foreign policy interests of the United States."

The question presented is:

Does a district court clearly and indisputably err in ordering production of sensitive technical documentation without applying the standards set forth in the parties' protective order and without considering the Executive Branch's national-security interests in the documentation at issue?

PARTIES TO THE PROCEEDING BELOW

Petitioners (defendants in the district court and mandamus petitioners in the court of appeals) are Micron Technology, Inc., and Micron Consumer Products Group, LLC.

Respondent in this Court is the United States District Court for the Northern District of California. Respondents also include Yangtze Memory Technologies Company, Ltd. and Yangtze Memory Technologies, Inc. (collectively, plaintiffs in the district court and real parties in interest in the court of appeals).

CORPORATE DISCLOSURE STATEMENT

Petitioners Micron Technology, Inc. and Micron Consumer Products Group, LLC are neither subsidiaries nor parent companies of any other corporation under the laws of the United States, and no publicly traded corporation owns 10 percent or more of their stock.

RELATED PROCEEDINGS

Yangtze Memory Technologies Company, Ltd. v. Micron Technology, Inc., No. 3:23-cv-05792 (N.D. Cal.) (order entered January 14, 2025)

In re Micron Technology Inc., No. 25-117 (Fed. Cir.) (order entered February 26, 2025)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules and Regulations

Other Authorities

INTRODUCTION

The discovery process in patent litigation requires production of sensitive information. Parties therefore routinely enter into protective orders that set rules for access to such information and set forth standards to be applied when disputes arise. The district court did not follow or enforce the parties' agreed-to rules, necessitating this petition.

Petitioners (collectively, "Micron") agreed to certain limits on the production of paper copies of its sensitive technical documents, including paper copies of its source code. Micron was concerned that corporate Respondents (collectively, "YMTC"), who were the plaintiffs below, would seek discovery beyond what was needed to litigate the case and try to gain access to Micron's technical documents for improper purposes. After all, the U.S. government had recently added YMTC to its Entity List, having determined, "based on specific and articulable facts," that YMTC poses "a significant risk of becoming involved in activities contrary to the national security or foreign policy interests of the United States." C.A. App. 363; *see* Additions and Revisions to the Entity List and Conforming Removal from the Unverified List, 87 Fed. Reg. 77,505, 77,505-08 (Dec. 19, 2022); 15 C.F.R. § 744.11(b). Micron's past experience with criminal theft of its technical information by entities similar to YMTC, coupled with the U.S. government's requirements that Micron exercise extra diligence in preventing YMTC from gaining access to sensitive technical information, justified Micron's concerns.

Micron thus insisted upon reasonable limits on access to technical information produced in discovery and demanded, and obtained, a reasonable process for resolving discovery disputes. Specifically, Micron persuaded the court below to include a provision in the protective order that required YMTC to show that any request to produce source code in paper copy form—the least secure of the inspection options available to the parties—was "reasonably necessary" to litigation preparation and not "excessive." And the district court endorsed these rules when it entered the parties' protective order.

When YMTC made a unique request for 73 pages of printed source code for Micron's most technologically advanced product, Micron invoked those requirements of the protective order. Micron explained that YMTC's request clearly was not "reasonably necessary" for the litigation. The request came many months before expert reports and summary judgment motions would be filed and before YMTC had noticed a single deposition, was more than 10 times larger than any prior request for paper copies of similar information for earlier-generation products, and targeted sensitive technical information about Micron's new generation of 3D NAND chips. But when Micron asked YMTC to justify its request for so much printed source code, YMTC failed to do so. And the district court declined to hold YMTC to its burden of overcoming Micron's objection. Instead, the district court applied a lower standard—mere relevancy—and ignored completely the national-security concerns tied up with YMTC's demands.

The district court failed to acknowledge the significance of deviating from the terms of the parties' protective order. Semiconductors power modern life, from smartphones and cars to the stock market and advanced weaponry. The United States and China, among others, have raced to develop robust domestic semiconductor industries to achieve their economic, military, and geopolitical goals. Given that context, confidential information about semiconductor technology is, by its very nature, tied up with important national-security and foreign-policy concerns. Indeed, in 2020, the Department of Justice secured convictions against a foreign entity that stole Micron's highly confidential technical documents—the same types of documents that YMTC sought paper copies of here.

The district court, ignoring its obligation to ensure the parties complied with the protective order, ordered Micron to hand over paper copies of its source code—to which fewer than a dozen of *Micron's* over 50,000 employees have full access. The Federal Circuit refused to correct that clear error. This Court's review is necessary to course-correct and ensure that the terms of the protective order are enforced.

OPINIONS AND ORDERS BELOW

The opinion of the United States Court of Appeals for the Federal Circuit is unreported and reproduced at Pet. App. 1a-6a.

The district court's order denying Micron's motion for relief from the magistrate judge's discovery

order is unreported and reproduced at Pet. App. 7a-8a.

The magistrate judge's discovery order is unreported and reproduced at Pet. App. 9a-15a.

JURISDICTION

The Federal Circuit entered judgment on February 26, 2025. *See* Pet. App. 6a. This Court has jurisdiction under 28 U.S.C. § 1651 or, in the alternative, 28 U.S.C. § 1254(1).

STATEMENT OF THE CASE

Micron and YMTC both manufacture 3D NAND semiconductor memory chips, an extremely valuable technology with important national-security implications.

Micron is an Idaho-based company that is a global leader in creating semiconductor technology. C.A. App. 87, 106. Founded in 1978, Micron operated for decades as the smaller player among international giants in the highly competitive market for semiconductor memory products. Today, Micron is the only U.S.-based manufacturer of semiconductor memory devices. C.A. App. 87-88.

For over a decade, Micron has been at the forefront of developing new and innovative 3D NAND memory products. C.A. App. 88. Micron's 3D NAND technology is the highest-density flash memory available. C.A. App. 257. Flash memory is the storage technology used inside laptops, data center servers, cellphones, and tablets. *Id.*

Micron devotes billions of dollars to technology and design innovation. In 2024 alone, Micron spent $3.43 billion on research and development. Micron, Annual Report Pursuant to Section 13 Or 15(D) of the Securities Exchange Act of 1934 for the Fiscal Year Ended August 29, 2024 at 48, https://tinyurl.com/Micron10K. This investment drives Micron's leading position in the market and gives Micron the ability persistently to lead the market with new generations (or "series") of 3D NAND products. C.A. App. 111.

For each generation of 3D NAND, Micron creates a confidential technical document called a "Traveler Presentation." C.A. App. 371. The Traveler Presentations contain key portions of Micron's source code and are treated as highly confidential technical documents. *Id.* For its most recent, most technologically advanced product on the market, Micron has a "150 Series Traveler Presentation." *Id.*

The semiconductor industry and Executive Branch know the value of these Traveler Presentations. In 2020, the Department of Justice announced a guilty plea in a case involving a Taiwanese company's theft of Micron's chip technology. *See* Press Release, U.S. Dep't of Justice, Taiwan Company Pleads Guilty to Trade Secret Theft in Criminal Case Involving PRC State-Owned Company (Oct. 28, 2020), https://tinyurl.com/5n76jbkb ("*DOJ Press Release*"). The Taiwanese company had conspired to steal Micron's trade secrets for the benefit of a Chinese state-owned enterprise. The theft included three of Micron's Traveler Presentations. *See* Indictment, *Unit-*

ed States v. United Microelectronics Corp., No. 18-CR-00465, Dkt. 1 (N.D. Cal. Sept. 27, 2018).

The Chinese government helped launch YMTC in 2016 to develop 3D NAND memory technology. Almost immediately, YMTC began a systematic and targeted effort to recruit Micron engineers who had worked on Micron's 3D NAND technology. C.A. App. 316-23, 363.

In 2022, the Department of Commerce placed YMTC on the Bureau of Industry and Security's Entity List.[1] C.A. App. 363; *see* 87 Fed. Reg. at 77,505-08; 15 C.F.R. § 744.11(b). Placement on the Entity List means the U.S. government determined, "based on specific and articulable facts," that YMTC poses "a significant risk of becoming involved in activities contrary to the national security or foreign policy interests of the United States." 87 Fed. Reg. at 77,505-08. One such activity is "[e]ngaging in conduct that poses a risk of violating the EAR [Export Administration Regulations]." 15 C.F.R. § 744.11(b)(1)-(5).

YMTC's placement on the Entity List requires third parties—like Micron—"to take extra due diligence" in dealings with YMTC, and critically, that caution extends to dealing with agents of YMTC. Bu-

[1] Housed under the Commerce Department, the Bureau of Industry and Security serves to "[a]dvanc[e] U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promot[e] continued U.S. strategic technology leadership." Bureau of Industry and Security, *About BIS*, https://tinyurl.com/3eyp62jm (last visited May 19, 2025).

reau of Industry and Security, *Policy Guidance FAQs*, https://tinyurl.com/ycxrx5wu (last visited May 19, 2025) ("*BIS FAQs*"). Notably, the Bureau of Industry and Security "considers that transactions of any nature with listed entities carry a 'red flag' and recommends that U.S. companies proceed with caution with respect to such transactions." *Id. at* https://tinyurl.com/24268fw8.

YMTC's activities continue to draw U.S. government scrutiny: In 2024, the Pentagon placed YMTC on a list of Chinese companies assisting China's military. U.S. Dep't of Defense, *Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283)* (Jan. 31, 2024), https://tinyurl.com/4usvptef; *see* Idrees Ali et al., *Pentagon Calls Out Chinese Companies It Says Are Helping Beijing's Military*, Reuters (Feb. 1, 2024), https://tinyurl.com/46j6hfpn.

YMTC sued Micron for patent infringement, and the parties entered a protective order governing access to sensitive discovery materials.

YMTC sued Micron in November 2023, alleging that multiple generations of Micron's 3D NAND products infringed YMTC's patents. C.A. App. 41-73. The parties jointly agreed to a protective order that sets out limitations on access to discovery, and the magistrate judge entered the order. As relevant here, the protective order includes procedures for reviewing highly sensitive source code materials. C.A. App. 273-78.

Per the protective order, parties' counsel, experts, and consultants may inspect source code on a specially protected source code review computer. C.A. App. 273-74. The computer is not connected to the Internet or to a printer and is stripped of extraneous software. *Id.* The reviewers may take notes about the source code and use those notes to develop litigation positions. C.A. App. 275-76. Inspections take place in a secure environment at counsel's office or at Micron's facilities. C.A. App. 364. YMTC had reviewed source code on a source code review computer more than 10 times by January 2025. C.A. App. 336, 345.

The protective order also provides that if a party wants "paper copies" of source code, it may request them. C.A. App. 276. These requests are limited, however, to only "portions of the materials" that are "reasonably necessary to facilitate … preparation of

court filings, pleadings, expert reports, or other papers, or for deposition or trial." *Id.*

The party producing source code (here, Micron) may object that the requested source code paper copies are "excessive" or "not reasonably necessary" to case preparation. *Id.* The requesting party (here, YMTC) bears the burden of overcoming any objection. C.A. App. 268. Once paper copies are produced, receiving counsel may each make six additional paper copies. C.A. App. 276.

Given the complexity and sophistication of Micron's chips, a potentially huge volume of source code may be relevant to the issues in dispute in this case. If all of Micron's source code describing its chips were printed, the source code would span millions of pages. Accordingly, the protective order placed a ceiling on the outer bounds of a request for a physical production of source code: no more than 1,500 pages total, and no more than 30 consecutive pages. C.A. App. 276. In addition to those quantitative limits on print outs, the protective order also set out the two qualitative limits described above, namely, that the paper copies must be "reasonably necessary" and "not excessive." Thus, the quantitative and qualitative limits are separate and independent hurdles for obtaining paper copies of source code.

YMTC demanded 10 times more printed pages of source code for Micron's latest-generation chips than it had for earlier-generation chips.

YMTC and Micron were successfully operating under the protective order until YMTC made an un-

precedented request. As noted, Micron had already made its source code available for inspection by YMTC's experts on a secured computer in counsel's office, a controlled environment. Following each of those inspections, YMTC requested *no more than 5 pages* of paper copies from the Traveler Presentations for the older 3D NAND generations. C.A. App. 365.

After an employee of YMTC's outside counsel conducted two inspections of Micron's Traveler Presentations, however, YMTC requested *73 pages* of the Traveler Presentation that describes Micron's latest generation products, the 150 Series. *Id.*

Ignoring the sensitivity of the material, its ability to readily inspect the material securely, and its status as a listed entity, YMTC insisted it needed paper copies of what amounts to *87%* of the substantive portions of the 150 Series Traveler Presentation. *Id.* For context, conservatively assuming only the 12 outside counsel who have appeared at the district court received those 73 pages, if each outside counsel made 6 copies (as the protective order permits), they would have *5,256 printed pages* of Micron's source code.

Micron objected to YMTC's demands, and the district court overruled Micron's objection.

Micron objected to YMTC's production request, arguing that YMTC's request was "excessive" and "not reasonably necessary [for] any case preparation." C.A. App. 336, 366. Micron emphasized that the protective order specifically provided safeguards

against handing over such a large portion of the 150 Series Traveler Presentation to YMTC's counsel, experts, and consultants in paper form, outside of a controlled, secure environment. C.A. App. 336-37; *see* C.A. App. 365, 373.

YMTC downplayed Micron's concerns and emphasized that its request was within the numerical limits provided by the protective order. C.A. App. 337. Its stated reason for requesting the printed production was the vague assertion that YMTC needed printed copies so the source code "can be cited in pleadings, expert reports, etc.," without citing any specific pleadings or reports. C.A. App. 338-39.

The magistrate judge granted YMTC's request in full. C.A. App. 3. The magistrate judge reasoned that YMTC's request was permissible because Micron did not dispute the pages' relevance and "the volume of the requested source code" was "within the presumptive limits" of the protective order's ceiling of 30 consecutive pages or 1,500 total pages. *Id.* The magistrate judge also pointed out that YMTC had excluded certain pages from its request, "such as title slides, summary slides, and background information" which, to the magistrate judge, "tend[ed] to demonstrate that YMTC's request [was] thoughtful and focused." *Id.* Finally, the magistrate judge quoted from a few provisions in the protective order to conclude that "strong protections" were in place to prevent unauthorized access to Micron's source code. *Id.*

Micron timely filed objections to the magistrate judge's order, emphasizing the national-security im-

plications and the magistrate judge's myopic focus on the protective order's numerical ceiling, and further argued that mere relevance did not justify the hard-copy production. C.A. App. 360-68.

The district court summarily denied the motion in a single-paragraph order. Pet. App. 7a-8a. The district court did not acknowledge or address any of the national-security concerns Micron brought to its attention. Nor did the district court explain how YMTC had met its burden of showing that its print request was reasonably necessary.[2] *Id.*

Micron petitioned for a writ of mandamus from the Federal Circuit, and the court denied the writ.

Micron filed a petition for writ of mandamus in the United States Court of Appeals for the Federal Circuit. The Federal Circuit denied the petition, stating that it was "not prepared to disturb the trial court's balancing of the interests on limited mandamus review based merely on Micron's conjecture that an individual might violate the protective order and subject themselves to appropriate sanctions." Pet. App. 6a.

Following the Federal Circuit's denial of mandamus, the district court stayed all deadlines pend-

[2] For ease of reference, mention of "the district court's order" going forward encompasses the magistrate judge's discovery ruling. *Cf. In re TikTok, Inc.*, 85 F.4th 352, 357 n.4 (5th Cir. 2023) (treating references to the district court's order as "synonymous" with references to the magistrate judge's order).

ing administrative proceedings in the United States Patent and Trademark Office. Micron has not yet produced any paper copies of the 150 Series Traveler Presentation.

REASONS FOR GRANTING THE WRIT

I. Micron's Right To Mandamus Relief Is Clear And Indisputable.

The issuance of a writ of mandamus is warranted when the party seeking the writ establishes that "(1) no other adequate means [exist] to attain the relief [it] desires, (2) the party's right to issuance of the writ is clear and indisputable, and (3) the writ is appropriate under the circumstances." *Hollingsworth v. Perry*, 558 U.S. 183, 190 (2010) (per curiam) (cleaned up). Micron has satisfied all three criteria. This case also implicates "a question of public importance." *See id.* (quoting *Ex parte United States*, 287 U.S. 241, 248-49 (1932)). Accordingly, this Court should issue a writ of mandamus directly to the district court.

In the alternative, Micron respectfully requests that the Court treat this petition as a petition for a writ of certiorari, grant the writ, and reverse the Federal Circuit's refusal to grant mandamus relief.

A. The district court clearly and indisputably erred by failing to justify its ruling and ignoring the unambiguous, mutually agreed-upon terms of the protective order.

The district court's order errs on its own terms. The court did not hold YMTC to its burden of overcoming Micron's objections and did not consider the parties' agreed-upon limitations on paper copies—that any request be reasonably necessary for litigation preparation and not excessive. Each failure was clear and indisputable error.

"Protective orders, like the ones the parties entered into here, are meant to prevent gamesmanship and provide for efficient resolution of discovery issues." *Moore v. Ford Motor Co.*, 755 F.3d 802, 811 (5th Cir. 2014) (Elrod, J., dissenting). Once parties agree to such rules, and the court endorses them, the parties should be held to their obligation to play by the rules. Yet here, the district court essentially modified the rules governing the parties' discovery as the process was unfolding.

"It is 'presumptively unfair for courts to modify protective orders which assure confidentiality and upon which the parties have reasonably relied.'" *AT & T Corp. v. Sprint Corp.*, 407 F.3d 560, 562 (2d Cir. 2005) (citation omitted). After all, "[a]n agreed protective order may be viewed as a contract, and once parties enter an agreed protective order they are bound to its terms." *Moore*, 755 F.3d at 809 (Elrod, J., dissenting) (citation omitted). And it is axiomatic that "[i]t is the province of courts to enforce con-

tracts—not to make or modify them." *The Harriman*, 76 U.S. 161, 173 (1869).

The district court impermissibly modified the terms of the protective order by failing to hold YMTC to its burden of persuasion—which it cannot meet.

1. The district court failed to enforce the terms of the protective order.

First, the district court did not hold YMTC to the agreed-upon burden of persuasion in the protective order. YMTC bore the burden of overcoming Micron's objection that YMTC's request for printed pages was excessive and not reasonably necessary. By failing to hold YMTC to its burden, the district court committed a legal error. *See Abbott v. Perez*, 585 U.S. 579, 607 (2018) ("whether the court applied the correct burden of proof is a question of law subject to plenary review"); *Addington v. Texas*, 441 U.S. 418, 425 (1979) ("even if the particular standard-of-proof … do[es] not always make a great difference in a particular case, adopting a 'standard of proof is more than an empty semantic exercise'" (citation omitted)). This makes sense: The standard of proof "serves to allocate the risk of error between the litigants and to indicate the relative importance attached to the ultimate decision." *Addington*, 441 U.S. at 423.

The protective order states that YMTC, as the requesting party, bears the burden of overcoming any objection. C.A. App. 268. YMTC did not even address the burden, let alone carry it, and the district court failed to hold YMTC to it. YMTC simply stat-

ed—and the district court accepted—that YMTC needed all 73 pages of source code in printed copy so the pages could "be cited in pleadings, expert reports, etc." C.A. App. 339.

This "justification" was plainly insufficient. The statement that YMTC needed printed copies to cite them in pleadings and expert reports is no better than saying the source code is relevant. Relevancy is not the standard for production of hard copies of the source code. YMTC did not identify any specific pleading or motion in which any pages—much less 73 pages—needed to be cited. The assertion that YMTC needed 73 pages to prove its infringement case appeared pretextual. To prevail on its patent-infringement claims against multiple generations of Micron 3D NAND products, YMTC must prove infringement of each generation separately. YMTC offered no explanation as to why 5 pages of a Traveler Presentation were sufficient for every generation except for the newest, most technologically advanced generation.

The request for paper copies therefore raised a "red flag" to Micron. *See BIS FAQs*. Take the expert reports. When YMTC made its request for the 73 printed pages in November 2024, expert reports were not due until October 2025—nearly a year away. YMTC offered no explanation as to why it could possibly need all 73 pages to prepare reports that weren't even due for eleven more months. YMTC's explanation "fail[ed] to show *both* the relevance of the requested information *and* the need for the material in developing its case." *In re Remington Arms Co.*, 952 F.2d 1029, 1032 (8th Cir. 1991) (em-

phasis added). YMTC's request was unjustifiably disproportionate to the needs of the case, especially at this early stage. YMTC never explained—and, crucially, the district court never held YMTC to its burden to explain—its reasoning for its excessive and unreasonable request. It follows that "there [was] no reason for the discovery request to be granted." *Id.* The district court's decision otherwise was clear error. This Court should thus follow its "usual practice" and instruct the district court to apply the correct burden of proof. *Cf. E.M.D. Sales, Inc. v. Carrera*, 604 U.S. 45, 54 (2025).

Second, the district court simply ignored the parties' mutually agreed-upon limitation that paper copies must be "reasonably necessary" to the litigation and not "excessive." In fact, the district court failed to extend its analysis beyond relevance at all. True, "[t]he Federal Rules of Civil Procedure permit broad discovery." *Bonner v. Triple-S Mgmt. Corp.*, 68 F.4th 677, 684 (1st Cir. 2023), *cert. denied*, 144 S. Ct. 1003 (2024). "[B]ut 'discovery, like all matters of procedure, has ultimate and necessary boundaries.'" *Id.* (quoting *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978)).

The district court gave no reason for ignoring the terms of the parties' agreed-to boundaries here. This is clear error. Indeed, it is black-letter law that "agreements voluntarily and fairly made shall be held valid and enforced in the courts." *Twin City Pipe Line Co. v. Harding Glass Co.*, 283 U.S. 353, 356 (1931). It follows that a court should only "occasional[ly] exercise[] judicial power to abrogate private agreements" in limited circumstances, such as if

an agreement is illegal or against public policy. *United Paperworkers Int'l Union, AFL-CIO v. Misco, Inc.*, 484 U.S. 29, 42 (1987). No such situation exists here. Rather, the protective order was the result of "an arm's-length negotiation by experienced and sophisticated" parties, so "it should be honored by the parties and enforced by the courts." *M/S Bremen v. Zapata Off-Shore Co.*, 407 U.S. 1, 12 (1972). The district court's failure to apply the mutually agreed-upon, unambiguous terms of the protective order was clear and indisputable error.

2. Had the district court held YMTC to its burden, YMTC could not have met it because the requested production was excessive and not reasonably necessary for case preparation.

Excessive. The district court's conclusion that YMTC's request was not excessive merely because it fell within the numerical limits of the protective order was clear and indisputable error: YMTC did not and cannot meet the qualitative limit in the protective order, which required YMTC to show its request was not excessive under the circumstances.

The protective order has independent quantitative and qualitative limits. The quantitative limits in the protective order are outer bounds, but falling within the quantitative limits says nothing about whether a request meets the qualitative standard prohibiting an excessive request. The district court failed to recognize that the two types of limits are independent, and its order effectively read out the

"excessive" limitation. A request is not excessive *only* if it exceeds the page limit; it can also be excessive if it is under the quantitative limit but qualitatively excessive.

The court did not "appreciate[] the potential harm from the disclosure of a firm's proprietary source code, even with the safeguards offered by a protective order." *In re Google Litig.*, No. 08-03172, 2011 WL 286173, at *5 (N.D. Cal. Jan. 27, 2011). Indeed, while "the protections set forth in" a stipulated protective order "are careful and extensive," nothing is "as safe as nondisclosure." *Viacom Int'l Inc. v. Youtube Inc.*, 253 F.R.D. 256, 260 (S.D.N.Y. 2008).

The district court also failed to consider, and YMTC cannot justify, the context of YMTC's request. A page limit for discovery of an entire universe of code should not be mechanically applied to a small—crucially important—portion of that universe. The 73 printed pages YMTC requested from the single Traveler Presentation amount to *87%* of the substantive pages of the document.

The district court and YMTC ignored the value and sensitivity of this source code. And YMTC never meaningfully explained why its request for printed copies was necessary. The fact that the U.S. government criminally charged parties for stealing Micron's Traveler Presentations shows the critical importance of the documents. *See DOJ Press Release*, https://tinyurl.com/5n76jbkb. The district court needed to at least consider and explain how YMTC had justified its need for paper copies.

Not Reasonably Necessary. The district court ignored that nothing in YMTC's arguments justifies requiring Micron to produce *this* source code in *this* format. YMTC's agents already had access to this source code in a secure format and had inspected the 150 Series Traveler Presentation multiple times on a secure source code review computer. It is simply not "reasonably necessary" for YMTC to obtain hard copies of 87% of the substantive portions of the 150 Series Traveler Presentation when YMTC was satisfied with a small fraction of that amount for earlier generation Presentations.

YMTC has *never* articulated a reason why the less secure hard-copy format is required for it to prepare its case. *See, e.g.*, *Synopsys, Inc. v. Atoptech, Inc.*, No. 13-cv-02965, Dkt. 846 at 3 (N.D. Cal. Sept. 16, 2016) (denying request for source code where requesting party made "no effort to tether its broad request for source code to specific purposes allowed under the Protective Order, nor [did the plaintiff] provide any explanation of why the amount of requested portions is 'reasonably necessary'"). And YMTC's past discovery behavior suggests it is *not* necessary—YMTC asked for a far narrower hard-copy production for all prior Traveler Presentations. If that narrower production was sufficient for earlier generations of products that are accused of infringement, it should also be sufficient for the current generation. The district court's failure to recognize that YMTC's request was not reasonably necessary for the litigation was clear error.

In short, the court "cannot abdicate its responsibility to oversee the discovery process." *Procter &*

Gamble Co. v. Bankers Tr. Co., 78 F.3d 219, 227 (6th Cir. 1996). Yet by deferring to the numerical limits in the protective order without interrogating YMTC's explanation, the district court abdicated its duty as the manager of discovery and failed to conduct a meaningful inquiry into whether YMTC's request was reasonably necessary to case preparation (it was not) or excessive (it was). This was clear and indisputable error.

B. The district court clearly and indisputably erred by disregarding the national-security and foreign-policy concerns at stake.

"This is not a routine discovery dispute." *Cheney v. U.S. Dist. Ct. for D.C.*, 542 U.S. 367, 385 (2004) (emphasizing separation-of-powers considerations in mandamus action). To the contrary, it implicates national-security and foreign-policy concerns in requiring the disclosure of Micron's sensitive documents in paper form to agents of a listed entity: a Chinese state-owned semiconductor company. In denying Micron's objections to the discovery order without any acknowledgement or explanation whatsoever of these national-security and foreign-policy risks, the district court ran afoul of its duty to "fully consider the factors relevant to [the] question" before it. *In re ZTE (USA) Inc.*, 890 F.3d 1008, 1010 (Fed. Cir. 2018) (granting mandamus). That was clear error.

From the start, Micron has explained that YMTC's request raises heightened security concerns

deserving of the court's careful attention.[3] C.A. App. 335-36. Micron further demonstrated the national-security implications of such documents. Notably, the Department of Justice had recently "secured a criminal conviction" against a Taiwanese company, which was acting in concert with a Chinese state-owned entity, "for stealing this kind of information from Micron."[4] C.A. App. 335. That conviction resulted in a criminal fine that was "the second largest ever in a criminal trade secret prosecution." *DOJ Press Release*, https://tinyurl.com/5n76jbkb.

Even a passing familiarity with the semiconductor industry is enough to recognize that these security concerns are part of the broader national-security and foreign-policy terrain. The U.S. government has limited foreign collaboration on semiconductor-technology development. Press Release, Dep't of Com., Biden-Harris Administration Announces Final

---

[3] Micron raised security concerns in its joint letter to the magistrate judge, C.A. App. 335-36, at the hearing before the magistrate judge, C.A. App. 344, and in its objections to the magistrate judge's order, C.A. App. 363.

[4] This Taiwanese company had cut a deal with a company created by the Chinese province of Fujian to develop memory devices and proceeded to recruit former Micron employees who brought with them highly sensitive Micron information—a "perfect case study of the state-backed intellectual property theft foreign companies operating in China had long complained of." Chris Miller, *Chip War: The Fight for the World's Most Critical Technology* 306-08 (2022). Here, Micron has filed counterclaims alleging that YMTC hired Micron engineers and filed patents in YMTC's name on ideas those engineers worked on while in Micron's employ. *See, e.g.*, C.A. App. 92-93, 318-24.

National Security Guardrails for CHIPS for America Incentives Program (Sept. 22, 2023), https://tinyurl.com/K2h3tUrX. More broadly, the United States has taken major steps to build up and protect its own semiconductor-technology infrastructure, including by enacting the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act in 2022, investing almost $53 billion "to bring semiconductor supply chains back to the U.S." Dep't of Com., *Two Years Later: Funding from CHIPS and Science Act Creating Quality Jobs, Growing Local Economics, and Bringing Semiconductor Manufacturing Back to America* (Aug. 9, 2024), https://tinyurl.com/33juesen.

Because it is highly dependent on imports of semiconductor parts, the United States is vulnerable to semiconductor supply-chain disruptions. Magnifying these vulnerabilities are China's competing—and nationalistic—ambitions with respect to its own semiconductor production. *See* Emily G. Blevins, Alice B. Grossman, & Karen M. Sutter, Cong. Rsch. Serv., R47508, *Semiconductors and the Semiconductor Industry* (2023), https://tinyurl.com/y22czv8k. Micron, of course, plays an outsized role in all of this, as the only U.S.-based manufacturer of semiconductor memory devices.[5] As a result, YMTC's failure to jus-

[5] In 2015, Chinese investor Tsinghua Unigroup (which was involved in getting YMTC off the ground) floated the idea of buying Micron for $23 billion, though its offer was rebuffed. Miller, *supra* note 4, at 267. As "[m]any industry experts" have noted, "China's best chance at achieving world-class manufacturing capabilities is in NAND production." *Id.* at 319. And for that reason, YMTC holds a special place in China's national-

tify its request, and the district court's rubber stamp on it, is no ordinary error in the discovery process; it is one of national-security consequence.

Viewed against that backdrop, the national-security risks in this case come into sharper focus. As Micron pointed out to the district court, the U.S. government had added YMTC to the Entity List in 2022. C.A. App. 363. That was significant because it meant the U.S. government deemed YMTC to present a significant risk of becoming involved in "activities contrary to the national security or foreign policy interests of the United States." C.A. App. 363 (quoting 87 Fed. Reg. at 77,506).

Because of that designation, Micron took very seriously its resulting duty to comply with the export regulations. *See* 15 C.F.R. § 744.11. Indeed, section 9(j) of the protective order expressly contemplates that requests for printed source code are "subject to … export control restrictions." C.A. App. 275-76. And YMTC cannot deny that its counsel, experts, and consultants are agents of YMTC, triggering Micron's obligation to treat the request—which YMTC has not proved and cannot prove is proper—as a "red flag" and to "proceed with caution." *See* CAFC Resp. Br. 19-20. So, for example, when YMTC brought patent suits against Micron in 2023 and 2024, Micron "exercised 'extra due diligence' to comply with the regulations." C.A. App. 363. Micron has also "exercised caution in allowing YMTC and its agents to possess

---

security landscape as China's leading producer of NAND memory. *Id.*

highly sensitive information outside of controlled environments," like source code review computers. *Id.* It is precisely that caution that animated the parties' protective order, and Micron's objection to the discovery order here.

There is no indication that any court even considered these national-security and foreign-policy risks. At bottom, the district court's one-paragraph order provided just two reasons for dismissing Micron's objections: (1) YMTC's request for 73 pages was below the 1,500-page maximum; and (2) the protective order has "sufficient procedures to prevent duplication or unauthorized access." C.A. App. 375. Neither remotely began to address the national-security and foreign-policy risks Micron raised before the district court.

II. Micron Has No Other Adequate Means Of Relief.

The district court's discovery order will require Micron to turn over to the agents of a Chinese state-owned chip manufacturer, in paper form, sensitive information about Micron's 3D NAND memory products, with no adequate justification. Once that production is made, it can never be undone. Mandamus is thus the only available avenue to Micron. "A discovery order … is interlocutory and non-appealable under 28 U.S.C. §§ 1291, 1292(a)(1) and 1292(b)." *In re Perez*, 749 F.3d 849, 855 (9th Cir. 2014) (citation omitted) (finding mandamus factors met for discovery order and granting petition); *see also Schlagenhauf v. Holder*, 379 U.S. 104, 109-12 (1964).

An ordinary appeal from final judgment is also an inadequate alternative. Because an order compelling Micron's hard-copy production of the requested materials "conclusively determine[s]" how the information will be provided to the opposing party, such an order is "effectively unreviewable on appeal from a final judgment." *In re Copley Press, Inc.*, 518 F.3d 1022, 1025 (9th Cir. 2008) (citation omitted).

Micron faces irreparable harm if forced to produce the paper copies of its source code. "Once the documents are surrendered pursuant to the lower court's order … [t]he status quo could never be restored." *Providence J. Co. v. FBI*, 595 F.2d 889, 890 (1st Cir. 1979); *see In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 761 (D.C. Cir. 2014) ("the cat is out of the bag") (Kavanaugh, J.) (citation omitted); *Agster v. Maricopa Cnty.*, 422 F.3d 836, 838-39 (9th Cir. 2005). That is because once YMTC's lawyers, experts, and consultants have access to the source code outside of the controlled environment of a source code review computer, Micron will no longer be able to track who has access to its source code, confirm proper destruction of copies, or control for human error.

Even under ordinary circumstances, "the chance of a leak increases as the number of people having access to information increases." *United Steelworkers of Am., AFL-CIO-CLC v. Auchter*, 763 F.2d 728, 743 (3d Cir. 1985). And this is not an ordinary case. The acknowledged national-security and foreign-policy implications of producing these materials to YMTC magnify this risk.

By contrast, even a full denial of YMTC's request for paper copies will result in minimal to no prejudice to YMTC. YMTC can simply continue to review Micron's 150 Series Traveler Presentation using the secure on-site inspection protocol.

III. Mandamus Relief Is Appropriate Under The Circumstances.

Although a writ of mandamus is extraordinary relief, it is appropriate here because of the "importance of the issues at stake" and the irreparable harm to Micron and the United States if relief is denied. *Hollingsworth*, 558 U.S. at 190. The district court's order authorizes access to Micron's source code without regard to the mutually agreed-upon, court-endorsed rules made against the backdrop of the United States' efforts to protect its national-security interests in the global semiconductor industry.

The district court's order effectively allows YMTC to use the civil-discovery process to gain an unfair commercial advantage it otherwise could not because of its status as a listed entity. *See, e.g.*, *Eagle Comtronics, Inc. v. Arrow Commc'n Lab'ys, Inc.*, 305 F.3d 1303, 1311-14 (Fed. Cir. 2002) (after receiving a pending patent application from plaintiff in discovery pursuant to a protective order, defendant's counsel filed the same application with the U.S. Patent and Trademark Office, passing it off as defendant's own application). Even though the parties agreed to certain rules to govern discovery, and the district court endorsed those rules, the district court never fulfilled its end of the obligation. The district

court never put YMTC to the task of justifying its request for hard copies of Micron's source code. If courts do not enforce the limits agreed to in protective orders, and simply rubber-stamp discovery requests as happened here, bad actors will be incentivized to use the courts to gain access to documents they have no justification to obtain.

This Court has explained that mandamus is appropriate when the lower court's "actions would threaten the separation of powers" or otherwise "interfer[e] with a coequal branch's ability to discharge its constitutional responsibilities." *Cheney*, 542 U.S. at 381-82; *see also Ex parte Peru*, 318 U.S. 578, 588 (1943) (lower court's actions would threaten the separation of powers by "embarrass[ing] the executive arm of the Government"). The United States' decision to place YMTC on the Entity List, to restrict export of items including semiconductor technology to YMTC, and to include YMTC on the Pentagon's list of Chinese companies that assist China's military, are ample indications of the Executive Branch's policy concerns. The district court, however, showed no regard for the underlying separation-of-powers principles at play. This Court should not allow the lower court's order to take effect before any judicial decisionmaker applies the proper standard of review to YMTC's discovery request and expressly considers the full scope of the national-security risks at stake.

CONCLUSION

The Court should grant this petition for a writ of mandamus.

Respectfully submitted,

Kamilyn Y. Choi
Brenna Ferris Neustater
ORRICK, HERRINGTON & SUTCLIFFE LLP
2100 Pennsylvania Avenue NW
Washington, DC 20037

Jared Bobrow
Jeremy Jason Lang
Diana M. Rutowski
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025

Elizabeth R. Moulton
Counsel of Record
ORRICK, HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105
(415) 773-5700
emoulton@orrick.com

May 23, 2025