No. 19-1010

IN THE

Supreme Court of the United States

ACTAVIS HOLDCO U.S., INC., ET AL.,

Petitioners,

v.

CONNECTICUT, ET AL.,

Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Third Circuit

MOTION FOR LEAVE TO FILE BRIEF FOR *AMICI CURIAE* AND BRIEF OF TWELVE COMPANIES AND ROBERT D. OWEN AS *AMICI CURIAE* IN SUPPORT OF PETITIONERS

ROBERT D. OWEN
COUNSEL OF RECORD
EVERSHEDS SUTHERLAND (US) LLP
900 N. Michigan Avenue
Suite 1000
Chicago, IL 60611-6521
(312) 724-9006
RobertOwen@eversheds-sutherland.com

Counsel for Amici Curiae

MOTION

Pursuant to Rule 37.2(b) of the rules of this Court, Robert D. Owen and the below-listed companies respectfully move for leave to file a brief as *amici curiae* in support of Petitioners in the above-captioned case:

Microsoft Corporation
GlaxoSmithKline PLC
American International Group, Inc.
Oppenheimer & Co., Inc.
American Electric Power Company, Inc.
Kason Industries, Inc.
3M Company
Oracle America, Inc.
Genentech, Inc.
Deere & Company
Baxter International Inc.
Equitable Holdings, Inc.

Amici tender their proposed brief with this motion.

Counsel for *amici* have provided notice and sought consent from all parties to this action. All Respondents who are Plaintiffs-Respondents below have given their consent, but we have not received consent individually from Respondents who are non-petitioning defendants, possibly because of the disruption of personal schedules that the COVID-19 virus is today causing in our country. No party has refused to give consent, but considering the number of parties and in the interest of time and efficiency, *amici* respectfully move for leave to file the proposed brief.

Amici corporations are regular litigants in the federal courts. *Amici* corporations and Mr. Owen, who is an ediscovery practitioner and litigator, are invested in the development of the Federal Rules of Civil Procedure and civil discovery jurisprudence. The Order of the Special Master and the District Court in this case (the "Order"), as affirmed 2-1 by the Third Circuit, deeply concerns *amici.* Specifically, the Order is the most recent, and most distressing, example of a growing trend whereby requesting parties seek access to massive amounts of data without the protection of a relevance review by the producing parties. *Amici* are concerned about their own rights as non-parties who might share confidential and proprietary information with Petitioners, and about the privacy rights of innocent bystanders whose personal and confidential information, wholly irrelevant to the dispute, will be produced to Plaintiffs-Respondents and accessed by opposing counsel, document review vendors, and potentially hackers or others with malevolent intentions. *Amici* have a substantial interest in protecting these privacy interests in the present dispute and in future litigation.

Amici respectfully submit that the attached brief setting forth their views will be helpful to the Court in its consideration of these important issues and request that the Court grant leave to file the brief tendered with the motion.

Respectfully submitted,

Robert D. Owen
COUNSEL OF RECORD
EVERSHEDS SUTHERLAND (US) LLP
900 North Michigan Avenue, Suite 1000
Chicago, Illinois 60611-6521
(312) 724-9006
RobertOwen@eversheds-sutherland.com

Stacey M. Mohr
Michelle McIntyre
EVERSHEDS SUTHERLAND (US) LLP
999 Peachtree Street, NE, Suite 2300
Atlanta, Georgia 30309-3996
(404) 853-8000
StaceyMohr@eversheds-sutherland.com
MichelleMcIntyre@eversheds-sutherland.com

Counsel to Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

RULES & STATUTES

OTHER AUTHORITIES

INTERESTS OF THE AMICI CURIAE[1]

Amici Curiae corporations are regular litigants all over the country:

Microsoft Corporation
GlaxoSmithKline PLC
American International Group, Inc.
Oppenheimer & Co., Inc.
American Electric Power Company, Inc.
Kason Industries, Inc.
3M Company
Oracle America, Inc.
Genentech, Inc.
Deere & Company
Baxter International Inc.
Equitable Holdings, Inc.

Amicus Curiae Robert D. Owen is a Partner at Eversheds Sutherland (US) LLP. He is a nationally recognized expert in e-discovery and an experienced litigator. He is President of the Electronic Discovery

---

[1] Pursuant to Rule 37.6, *Amici Curiae* state that no counsel for a party authored this brief in whole or in part, and no person or entities other than *Amici Curiae*, their members or counsel made a monetary contribution to the preparation of submission of the brief. Counsel for *Amici Curiae* provided the requisite 10 days' notice to all parties and received consent from Petitioners, State Attorney General Respondents, Direct Purchaser Respondents, End-Payor Respondents, Indirect-Reseller Respondents, and Direct Action Respondents as well as some but not all of the Respondents who are non-petitioning defendants.

Institute and editor-in-chief of EDI's *The Federal Judges' Guide to Discovery* (3rd ed. 2017).

Amici respectfully submit this brief in support of Petitioners Actavis Holdco, Inc., *et al.* urging this Court to grant Petitioners' petition for certiorari seeking review of the decision of the United States Court of Appeals for the Third Circuit. That court improperly held, 2-1, that the district court could order Petitioners to produce irrelevant information via a flawed, one-round keyword search methodology that (i) gathered a vastly overinclusive collection of emails containing search term "hits" and (ii) *prohibited* Petitioners from removing irrelevant emails prior to production, the latter being the central error and clear departure from decades of practice to the contrary.

All *amici* defend claims all over the Nation, and some are seeing an increasing prevalence of requests to produce all documents in custodians' email accounts, or at least those containing keyword search terms. There is also a real danger that the confidential and valuable commercial information of some *amici* will exist in the document productions of defendants pursuant to the Order. All *amici* are deeply concerned about the effect of this ruling on actions in which they are parties, view the Order at issue here with alarm, and respectfully urge herein that the Court arrest this trend's progress.

SUMMARY OF THE ARGUMENT

Amici Curiae urge the Court to take up a recurring issue that has arisen because of the data explosion of the last few decades**:** Can parties be ordered to produce – in violation of the plain limitations of Rule 26(b)(1) – vast collections of documents without being afforded the opportunity to remove their own – and third parties' – irrelevant personal, private, trade secret, or confidential material?

Our Nation's system of full pretrial disclosure – so idealistic and workable in 1938 when the transformative Federal Rules of Civil Procedure were adopted – never anticipated a reality in which potentially disclosable material in a civil action could comprise millions or billions of pages. Nor could the architects of full disclosure have anticipated that properly discoverable documents might exist *literally alongside* and intermingled with irrelevant material containing commercial information of extraordinary value to parties as well as nonparties, or the highly personal information of nonparties who are but bystanders to the dispute.

Over time, the evolving reality of astronomical data volumes required courts, lawyers, and parties to adapt discovery practices to the new reality. Modes of coping came into being, a central tenet of which is that producing parties have the right and a reasonable opportunity to identify and remove irrelevant documents or content from collections of materials being produced to requesting parties.

Full pretrial discovery is of course a necessary component of our system for resolving civil disputes, but it comes at a cost, sometimes to the personal privacy of individuals and the confidential information of businesses. We tolerate the cost because it facilitates the peaceful resolution of civil disputes, but discovery is made subject to strict limiting rules to ensure that no more privacy is compromised than necessary. Our "civil tribunals . . . must be governed by sound rules of practice and procedure." Roberts, C.J., "2015 Year-end Report on the Federal Judiciary," at 2 (comparing our civil justice system to the "inherently uncivilized" practice of dueling). The instant case brings Chief Justice Roberts' admonition into sharp focus.

The district court order at issue (the "Order") requires defendants to produce every single email of hundreds of custodians that contain any one of hundreds of keyword search terms. Keyword searching of the type ordered here is an accepted method for pulling *potentiall*y responsive documents from a large collection of data. Yet, it is also well accepted that keywords inevitably pull huge volumes of emails having no connection to the case that, of course, contain much irrelevant information. Keyword hits and relevance "are not synonymous."[2] "Search terms are an important tool parties may use to identify *potentially* responsive documents in cases involving substantial amounts of ESI. Search terms do

---

[2] *Youngevity Int'l Corp. v. Smith*, No. 16CV00704, 2017 WL 6541106, at *10 (S.D. Cal. Dec. 21, 2017).

not, however, replace a party's requests for production,"[3] which must be stated with specificity in the first instance. [4]

In one recent study conducted by the National Institute of Standards and Technology ("NIST"), an agency of the U.S. Commerce Department, even the most carefully designed keyword search achieved only 44.6% precision, meaning 55.4% of the "hits" were nonresponsive.[5] While keyword searches of the type specified in the Order are commonly used in modern litigation, because of their imprecision as evidenced by the NIST study, they are only the first step in a methodology that also *requires* a substantive review of the "hits" to separate relevant information from the many false-positive retrievals. The Order improperly omits this critical step from the keyword methodology

---

[3] *Id.* (citing *In re Lithium Ion Batteries Antitrust Litig.*, No. 13MD02420, 2015 WL 833681, at *3 (N.D. Cal. Feb. 24, 2015) (keyword searches "often are overinclusive, that is, they find responsive documents but also large numbers of irrelevant documents.")

[4] *See* Fed.R.Civ.P. 34(b)(1)(A) ("The request: must describe with reasonable particularity each item or category of items to be inspected."); *Caves v. Beechcraft Corp.*, Case No. 15-CV-125, 2016 WL 355491 (N.D. Okla., Jan. 29, 2016) (denying motion to compel and sustaining defendant's objections to document requests that do not identify with reasonable particularity what is being sought because: "Neither Defendants nor the Court should have to guess what Plaintiff is really seeking.")

[5] Kirk Roberts, et al., "Overview of the TREC 2018 Precision Medicine Track," Text Retrieval Conference, https://trec.nist.gov/pubs/trec27/papers/Overview-PM.pdf (last accessed Mar. 15, 2020.)

and flies in the face of studies like NIST that prove keywords without a substantive review of "hits" actually identify as much – or more – irrelevant information as relevant: in the NIST study, the median precision of *all* searches was 26.7%, so that 73.3% of the material tagged by search terms was irrelevant.[6]

Egregiously, and of urgent concern to these *amici,* the Order forbids the producing parties from removing any non-responsive emails from those to be produced to plaintiffs-respondents, so that "[t]here is no dispute that the order compels the production of a volume of non-responsive and irrelevant emails."[7]

The Order thereby disregards the discovery limits of FED. R. CIV. P. 26(b)(1), and requires production of documents and information concededly unnecessary for the resolution of the dispute, undoubtedly including material in emails that the senders thought would remain forever private: e.g., trade secrets, personal health information protected by HIPAA, Social Security numbers, expert consultants' communications and reports, login and password credentials, valuable personally identifiable information, or even intensely personal, amorous communications. Under the Order, all of this material must be produced to plaintiffs and be exposed to innumerable persons at plaintiffs' law firms and document review vendors, not to mention any

---

[6] *Id.*

[7] *In re Actavis Holdco U.S., Inc.*, No. 19-3549 (3d Cir. Dec. 6, 2019)(order denying mandamus) (Phipps, J., dissenting).

malevolent hackers who may gain access to their data stores.[8] *Amici*'s proprietary and confidential information may also be included in that production.

As an article concerning this case published recently by *Forbes* states, "Employees' private conversations, personal business transactions, and financial data, irrelevant for the lawsuits but otherwise potentially compromising, could show up in produced emails."[9] This presents a severe problem for nonparty entities such as *amici*, not to mention the parties to this case and individual persons. The sweep of the Order also compromises the ability of our civil litigation system to coexist with the personal privacy regimes of other countries, most notably in the European Union.

Requests by plaintiffs for unfiltered production of data stores are becoming widespread nationally. Consequently, five other circuits have granted mandamus of similar orders – having found that expanding the scope of discovery is not within the

---

[8] It is now generally understood that law firms are particularly vulnerable to data breaches and are being specifically targeted for attacks. J. Randolph Evans and Shari L. Kleven, *Cybersecurity: You Can't Afford to Ignore It Anymore*, DAILY REPORT at 1 (Apr. 25, 2016) (noting U.S. Department of Justice investigation in wake of Russian hacker attacks on 48 law firms and aftermath of the Panama Papers hacking attack), available at http://tiny.cc/u2x3kz.)

[9] Glenn Lammi, "Supreme Court Must Take Action on Lawless Discovery Order in Generic-Drug Antitrust MDL," FORBES (March 6, 2020), https://tinyurl.com/se5crdr.

discretion of the district court[10] – and none have allowed such orders. The Order represents by far the most expansive application of this developing discovery thrust and if left in place it will inevitably encourage more such attempts in matters large and small.

As national conceptions of personal privacy evolve and tighten, and requests for unfiltered productions of confidential business information become more prevalent, the need grows for clarity around the production of personal or otherwise confidential emails in civil action pretrial discovery. Review of the Order by this Court is urgently needed.

ARGUMENT

I. WHY IS THE ORDER AND OTHERS LIKE IT SO CONCERNING TO *AMICI CURIAE*?

The Order is far from a "mere discovery order" unworthy of review by this Court, as Respondents suggest. Respondents Opp. to Stay, at 1. It threatens real harm to non-parties such as *amici*, parties, and individuals that protective orders cannot prevent, and typifies a growing trend of openly seeking production

---

[10] FED. R. CIV. P. 26(b)(2)(C) states unequivocally that "the court must limit . . . discovery [that] is outside the scope permitted by Rule 26(b)(1)." This was echoed by the dissent in the Third Circuit: "nothing in the civil rules permits a court to compel production of non-responsive and irrelevant documents at any time." App. D at 3 n.1

of irrelevant material. The Order and others like it should be decisively rebuffed now.

A. The Order and Others Like It Threaten Real Harm to the Proprietary and Privacy Interests of *Amici Curiae*.

In the normal course of their businesses, *amici curiae* companies, like all companies, regularly exchange with other entities highly confidential and valuable information via email. Because of (i) the excessive sweep and inherent limitations of one-round keyword searching, (ii) the fact that the emails of literally hundreds of custodians will be searched, and (iii) the fact that the producing parties are forbidden from removing irrelevant emails from the productions the Order requires them to make, there is real danger that some of the nonparty *amici*'s confidential and valuable commercial information will exist in the document productions of defendants pursuant to the Order.

Thus, the procedure specified in the Order could lead to the unnecessary production in this case and others of irrelevant but valuable trade secrets and other confidential information (e.g., confidential pricing, bank account credentials and information, financial statements). *See, e.g.*, *Sanderson v. Winner*, 507 F.2d 477 (10th Cir. 1974) (mandamus in antitrust action to prevent disclosure of private financial records). To make matters worse, the third parties such as *amici* may never discover that their proprietary and confidential information was disclosed.

Although the producing parties have a limited period of time within which to clawback emails they claim are irrelevant, nonparties including *amici* (i) will have no role at all in selecting emails for clawback and (ii) even if ultimately clawed back their proprietary and confidential information will have been exposed to all parties in this MDL for a period of time. In *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 35 (1984), the Court recognized that incidental release of third parties' irrelevant information could damage their privacy interests, and courts' processes should be managed to prevent such abuse:

> "[R]elevant information in the hands of third parties may be subject to discovery.
>
> "There is an opportunity, therefore, for litigants to obtain — incidentally or purposefully — information that not only is irrelevant but if publicly released could be damaging to reputation and privacy. The government clearly has a substantial interest in preventing this sort of abuse of its processes."

Moreover, parties do not have standing to protect proprietary or confidential business information of third parties, *see Burton Mech. Contractors, Inc. v. Foreman*, 148 F.R.D. 230, 234 (N.D. Ind. 1992) (collecting cases), so it is up to those third parties, like *amici* here, or the courts to protect those privacy interests.

B. The Order and Others Like It Threaten Real Harm to the Privacy Interests of Companies and Individuals Unrelated to the Action.

It is undeniable that individuals across all businesses routinely use their business email accounts to send personal material to others. Social Security numbers, logins and passwords, protected health information, even amorous communications – there is an endless list of sensitive information that can be found in business email repositories. The Court has noted, in discussing the new era of electronic communication, that "many employers expect or at least tolerate personal use of [electronic communication] equipment by employees because it often increases worker efficiency." *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759 (2010).

Producing any and all "hits" resulting from hundreds of search terms applied to hundreds of custodian email accounts ensures that there will be production of the custodians' highly personal, sensitive, and revealing emails to strangers they will never know.[11] The custodians' email correspondents –

---

[11] *Keywords Cannot Prevent Private or Protected Information From Being Retrieved.* Keyword searching like that at issue here is designed to assemble an overinclusive set of data from which responsive material can be pulled and produced, but it is not designed to *prevent* nonresponsive or private material from appearing in the tagged data set. A simple Google search (which is simply a keyword search like that at issue here) using just one of the hundreds of search terms proposed (*see* App. H to Petitioners Application for Stay Pending Certiorari) quickly makes concrete how innocent-sounding keywords can lead to

third parties outside the producing party as well as countless employees within it – will also have their emails exposed to anonymous persons. *See, e.g.*, *In re Ford Motor Co.*, 345 F.3d 1315, 1316 (11th Cir. 2003) (mandamus "[i]n the context of discovery orders" is appropriate to prevent "invasion of privacy rights."); *U.S. ex rel. Chandler v. Cook Cty., Ill.*, 277 F.3d 969, 981 (7th Cir. 2002) (mandamus appropriate to prevent "serious harm to patients' privacy rights"). The more copies of this valuable or private data that are distributed widely, the more chances there are for it to be accessed without authorization, or in the present age of hacking, simply stolen.

Protecting the privacy of employee data is increasingly important for *amici* companies and others. California recently enacted the California Consumer Privacy Act (CCPA), a sweeping privacy law that echoes the EU's GDPR and regulates companies' use of personal data. CAL. CIV. CODE § 1798.175. The CCPA is likely only the first of many such laws to come in the United States intended to protect the personal and private data of individuals.[12]

---

documents that are embarrassing and could lead to the inadvertent release of private information. For example, searching on one of those search terms, "play nice," returns a variety of websites, including many having pornographic overtones.

[12] New York, Nevada, and Massachusetts are among the many states enacting data privacy legislation. Michael Bahar, et al., *The state of US data privacy and cybersecurity laws in 2019* (updated Dec. 2019), https://us.eversheds-sutherland.com

Broad discovery orders, like the Order here, contravene the purpose of regulations like the CCPA and the growing trend of protecting privacy rights, hamper companies' compliance with statutes like the CCPA, and subject them to penalties. CAL. CIV. CODE § 1798.155.

Discovery is a serious intrusion into the privacy rights of the parties as well as others having nothing to do with the dispute. As a society, we allow it because it is necessary for the truth-seeking needs of the judicial system, but it necessarily has its carefully crafted limits and they should be respected. The Order does not do so.

C. The Mere Entry of a Protective Order Does Not Protect Against the Theft of Valuable Information Resident in Produced Emails.

The mere entry of protective orders does not protect against cybersecurity breaches or other risks of disclosure or misuse.[13] Moreover, such orders do not ensure there will be no disloyalty among document

---

/NewsCommentary/Articles/227590/The-state-of-US-data-privacy-and-cybersecurity-laws-in-2019.

[13] *See, e.g.,* David Kessler, et al., *Protective Orders in the Age of Hacking,* N.Y.L.J., Mar. 16, 2015 ("As discovery has become predominately digital, producing parties must now face the threat of third parties stealing highly sensitive information not just from their and their advisor's computer systems, but their opponents' data systems as well.").

reviewers given access to the documents produced pursuant to the Order.

The cybersecurity risk is real. At a time when even blue chip corporate law firms –e.g., Cravath and Weil Gotshal[14] – have been hacked and bad actors worldwide are continuing relentlessly to target major US entities, the risks that a sensationalistic target like personal emails of hundreds of custodians will be vulnerable to hacking secure should not be underestimated.[15]

Nor does the 120-day clawback feature ameliorate any of the foregoing risks. Rule 26 strictly forbids the production of irrelevant material because requesting parties and their counsel, like the Petitioners, are not entitled even to see such material, and once seen, the

---

[14] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J., Mar. 29, 2016.

[15] In addition, at a time when partisan political emotions are particularly pronounced, there can be no guarantee that every one of the dozens of persons given access to the personal information of the defendants' custodians will honor their obligation to preserve confidentiality if the reviewer opposes what he or she comes to learn about the custodian's political views while reviewing emails. *See, e.g.*, Alistair Barr, *Mozilla CEO Brendan Eich Steps Down*, WALL ST. J. (Apr. 3, 2014) (Mozilla CEO steps down following criticism over political donation); Katherine Rosman, *They Paid $42 for a SoulCycle Ride, Not for Trump*, N.Y. TIMES (Aug. 8, 2019), https://www.nytimes.com/2019/08/08/us/politics/soulcycle-equinox-boycott.html (customers boycott and fitness chains do damage control after news of stakeholder holding fundraiser for President Trump).

bell cannot be unrung.[16] A clawback procedure does not cure or mitigate this error.

D. The Order and Others Like It Threaten Conflict With Foreign Data Production Laws and Real Harm to International Relations.

The Order creates even more harm because Petitioners include multinational companies that do business globally. Not only does this mean that Petitioners do confidential business outside the United States that is irrelevant to the claims and defenses of the instant matter, but they have employees, vendors and clients who live and operate outside the United States and who of course communicate by email with colleagues in this country. The personal information of some of these employees, vendors, and clients will be protected by non-U.S. data protection laws, such as the European Union's General Data Protection Regulation (GDPR), that can conflict with United States discovery. *See. e.g. Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522 (1987).

It is already difficult for businesses to comply with their discovery obligations in U.S. courts while complying with their data protection obligations

---

[16] This is all the more problematic as, increasingly, the larger firms bring a larger share of class actions. Their exposure to irrelevant, confidential information, which cannot be erased from their minds, cannot be waved away as inconsequential.

abroad. *See generally.*, The Sedona Conference*, International Principles on Discovery, Disclosure & Data Protection in Civil Litigation.*[17] Compelling the unnecessary production of admittedly irrelevant documents almost certainly conflicts with the GDPR because the legitimate interest in producing irrelevant information arguably does not outweigh the data subject's interest in not having its personal information disclosed.[18]

Allowing the discovery practice ordered by the District Court to become prevalent would surely risk further disapproval of our practices and exacerbate issues of international comity. As this Court stated in *Aerospatiale*:

> "American courts . . . should exercise special vigilance to protect foreign litigants from the danger that unnecessary, or unduly burdensome, discovery may place them in a

---

[17]https://thesedonaconference.org/publication/International_Litigation_Principles (last visited Mar. 15, 2020).

[18] The fact the company is required to produce the irrelevant personal information under court order does not necessarily resolve the conflict and protect the business from sanction under E.U. law. *See* Samantha Cutler, *The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information*, 59 B.C. L. REV. 1513, 1524-32 (2018) (describing conflict between scope of federal discovery and expanding use of sanctions for data privacy breaches in Europe); *In re Air Cargo Shipping Servs. Antitrust Litig.*, 278 F.R.D. 51, 54 (E.D.N.Y. 2010) (compelling production despite potential sanctions under French discovery blocking statute).

> disadvantageous position. Judicial supervision of discovery should always seek to minimize its costs and inconvenience and to prevent improper uses of discovery requests. When it is necessary to seek evidence abroad, however, the district court must supervise pretrial proceedings particularly closely to prevent discovery abuses. . . . Objections to "abusive" discovery that foreign litigants advance should therefore receive the most careful consideration."

Id. at 546. Discovery in the federal courts is already considered very broad by those outside the United States, The Sedona Conference, *Practical in-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397, 407 (2016) ("Some civil law countries also have enacted blocking statutes to curb the broad reach of discovery from the U.S."), but parties have always been able to defend it by arguing that only documents probative to the dispute will be produced and parties will be able to minimize the impact on the data protection rights of non-U.S. data subjects. The Order sharply undercuts that defense.

II. THE ORDER CONTRAVENES EXISTING RULES IN MULTIPLE WAYS.

A. FED. R. CIV. P. 26(b)(1)

The Advisory Committee on Rules of Civil Procedure has responded to the explosion in data volumes by proposing, in successive steps over several decades, to narrow the scope of discovery set forth in

this rule, and the Court has adopted those proposals. This occurred in 1983, 1993, 2000 and 2015.

Rule 26(b)(1) now defines the proper scope of discovery more carefully than ever:

> "Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case. . . ."

As the first clause makes clear, Courts have the express power to "limit" discovery further, but the Rule does not grant district courts the power to *expand* the scope of what must be produced to a requesting party. In fact, the rule is explicit that "the court *must* limit . . . discovery [that] is outside the scope permitted by Rule 26(b)(1)." FED. R. CIV. P. 26(b)(2)(C)(emphasis supplied).

Not only are parties not entitled to irrelevant documents, they are not even entitled to all *relevant* documents as discovery is further limited by privilege and proportionality. The 2015 amendments expressly inserted the proportionality factor ("and proportional to the needs of the case") into the rule's primary definition of the scope of relevance, emphasizing anew the need to restrain disproportionate discovery. In requiring the production of innumerable irrelevant documents, which inevitably increases the costs of managing the larger resulting data set, the Order also mandates the production of disproportionate volumes of data, and thereby imposes significant unnecessary costs on the petitioners. "Rule 26(b)(1) crystalizes the

concept of reasonable limits on discovery through increased reliance on the common-sense concept of proportionality." Roberts, C.J., "2015 Year-End Report on the Federal Judiciary," at 6.

Discovery is not an end in itself, but merely a means of obtaining facts so that all parties have reasonably sufficient information to advocate their case and resolve disputes. Discovery is costly, not just in money, time and resources, but in its invasion of the privacy of parties and third-parties. We accept these costs and invasions because they help uncover truth and resolve disputes on their merits, but these costs inherently rein in the scope of discovery. It may seem that the most obvious example of these limits is proportionality, where the court weighs the expected value of the discovery against its expected costs, but the bright-line rule against the compelled production of irrelevant documents is the most important. *Schlagenhauf v. Holder*, 379 U.S. 104 (1964) ("The Federal Rules of Civil Procedure should be liberally construed, but they should not be expanded by disregarding plainly expressed limitations.") As irrelevant documents add nothing to resolving disputes, the costs to privacy, confidentiality and resources are balanced by nothing, and should never be required.

The Order is impermissible under these provisions of Rule 26, as are others like it. Attempts to erode the bright line rule against compelled production of irrelevant documents should be decisively rejected.

B. FED. R. CIV. P. 34(b)

In two ways, the Order is also inconsistent with Rule 34, governing the production of documents.

Option To Produce Specific Documents. In 2015, Rule 34(b)(2)(B) was amended to make express what was well-established, by adding the following language: "The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection." This addition was adopted "to reflect the common practice of producing copies of documents or electronically stored information rather than simply permitting inspection."[19] As the recently revised rule makes clear, the responding party has complete discretion to select and produce its responsive documents instead of allowing inspection of the documents.

"Production" in the context of this rule is where a responding party takes reasonable steps to identify responsive, relevant, and non-privileged documents from its corpus of information and provides copies to the requesting party. "Inspection," on the other hand, is where a responding party proffers an appropriately encompassing selection of documents where it believes the responsive, relevant and non-privileged documents are likely to reside and allows the requesting party to review them and identify the documents it believes it is entitled to receive. Inspections are generally less expensive for the responding party, because they don't require as much

---

[19] Committee Notes on Rules – 2015 Amendment.

time and expense to arrange, but the trade-off is that they allow access to irrelevant documents.

Seen in this light, the Order is clearly a compelled inspection, as the responding party has lost the right to exclude irrelevant documents, and contravenes the rule. The mere fact that the inspection is limited by certain custodians and certain search terms is a fig leaf. First of all, the search terms are not formulated to *exclude* personal and confidential emails. Second, when utilized, the inspection method never affords access to a responding party's entire facility or its complete set of documents. Some initial selection is always made, and here that is akin to the use of keyword search terms. A court cannot deprive a responding party of the Rule's alternative right to produce rather than allow inspection, absent evidence of serious discovery abuse, which is concededly not present here.

Obligation on Requesting Party To Make Particular Requests. One of the very few obligations on requesting parties is that they must "describe with reasonable particularity each item or category of items to be inspected." FED. R. CIV. P. 34(b)(1)(a). This is an important requirement; it protects responding parties from vague and ambiguous requests that either in their ambiguity sweep too broadly or, in the hands of less scrupulous requesting parties, support motions to compel seeking sanctions for failing to produce documents the responding party did not even understand were requested. This rule, accordingly, requires the requesting party to identify particularly what it needs. Once it does so, the rule requires the

responding party to do a reasonable search to find and produce those documents.

As clearly demonstrated by the district court's memorandum explaining its Order (Petition for Cert., App. C, at 16a, et seq.), the Order contravenes this requirement by relieving Respondents of the obligation to make specific requests and instead compels the production of irrelevant documents. The apparent motivation behind allowing this compelled inspection was the court's fear that the defendants would not understand the relevance or responsiveness of certain of their own documents. Respondents Opposition to Stay, at 5-7. However, it is incumbent on the requesting party to put "a 'reasonable person of ordinary intelligence' on notice of which specific documents or information would be responsive to the request." *Regan-Touhy v. Walgreen Co.*, 526 F.3d 641, 649–50 (10th Cir. 2008) (quoting Wright & Miller, 8A FEDERAL PRACTICE AND PROCEDURE § 2211, at 415) ("Though what qualifies as 'reasonabl[y] particular' surely depends at least in part on the circumstances of each case, a discovery request should be sufficiently definite and limited in scope that it can be said 'to apprise a person of ordinary intelligence what documents are required and [to enable] the court . . . to ascertain whether the requested documents have been produced.'").

Thus, if the Petitioners cannot understand what is relevant and responsive, then it is incumbent on Respondents to identify with more particularity what they are seeking. The Order improperly transfers the burden from Respondents to the Petitioners by forcing

them to produce irrelevant documents instead of the Respondents better identifying the information they need.

III. CERTIORARI IS URGENTLY NECESSARY.

Respondents attempt to portray this matter as a "mere discovery dispute" but the Order's extra-ordinary implications transcend the issues in the instant matter and go to the heart of our system for resolving civil disputes.

Respondents argue that this is a fact-bound dispute unworthy of review by this Court, and in any event the Order is well within the discretion of the district court. But the Order transgresses what had been a bright line: absent discovery misconduct, which is not shown here, Rule 26(b)(1) does not authorize orders to produce material outside that rule's scope of discovery.

Appeals to the district courts' discretion to enter such orders must remain unavailing. Just as a district court has no discretion to compel discovery on claims that fail as a matter of law, it also lacks discretion to order the production of irrelevant information.

CONCLUSION

For the foregoing reasons, this Court should grant Petitioners' petition for certiorari seeking review of the decision of the Court of Appeals for the Third Circuit.

Respectfully submitted,

Robert D. Owen
COUNSEL OF RECORD
EVERSHEDS SUTHERLAND (US) LLP
900 North Michigan Avenue, Suite 1000
Chicago, Illinois 60611-6521
(312) 724-9006
RobertOwen@eversheds-sutherland.com

Stacey M. Mohr
Michelle McIntyre
EVERSHEDS SUTHERLAND (US) LLP
999 Peachtree Street, NE, Suite 2300
Atlanta, Georgia 30309-3996
(404) 853-8000
StaceyMohr@eversheds-sutherland.com
MichelleMcIntyre@eversheds-sutherland.com

March 16, 2020