No. 14-1481

IN THE

Supreme Court of the United States

KELLY M. RINDFLEISCH,
Petitioner,

v.

STATE OF WISCONSIN,
Respondent.

On Petition for Writ of Certiorari to the Court of Appeals of the State of Wisconsin

BRIEF OF THE DKT LIBERTY PROJECT AND THE CATO INSTITUTE AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

ILYA SHAPIRO
CATO INSTITUTE
1000 Massachusetts Ave. NW
Washington, DC 20001
(202) 842-0200
ishapiro@cato.org

LINDSAY C. HARRISON
Counsel of Record
JULIA M. CARPENTER
MATTHEW E. PRICE
ELIZABETH C. BULLOCK
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
lharrison@jenner.com

Counsel for Amici Curiae

July 13, 2015

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS AND STATUTES

OTHER AUTHORITIES

INTEREST OF *AMICI*[1]

The DKT Liberty Project. Thomas Jefferson warned that "[t]he natural progress of things is for liberty to yield, and government to gain ground." Letter from Thomas Jefferson to Edward Carrington (May 27, 1788). Mindful of this trend, The DKT Liberty Project was founded in 1997 to promote individual liberty against encroachment by all levels of government and to defend the right to privacy. This not-for-profit organization advocates in favor of vigilance over regulation of all kinds, especially restrictions of individual civil liberties that threaten the reservation of power to the citizenry that underlies our constitutional system. The DKT Liberty Project is also particularly involved in defending the right to privacy, one of the most profound individual liberties and a critical aspect of every American's right (and responsibility) to function as an autonomous and independent individual.

The Cato Institute. Cato was established in 1977 as a nonpartisan public policy research foundation dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Center for Constitutional Studies was

---

[1] All parties have been timely notified of the undersigned's intent to file this brief. Both Petitioner and Respondent consented to the submission of this brief; their letters of consent are on file with the Clerk. Pursuant to Rule 37.6, none of the parties or their counsel authored this brief in whole or in part and no one other than *amici* and their counsel contributed money or services to the preparation of this brief.

established in 1989 to promote the principles of limited constitutional government that are the foundation of liberty. Toward those ends, Cato publishes books and studies, conducts conferences, issues the annual *Cato Supreme Court Review*, and files amicus briefs with the courts.

This case concerns the protections that the Fourth Amendment provides to what often is the most personal of an individual's electronic data: email. The lower court here disregarded the fundamental restraints that the Fourth Amendment places on the government's right to rummage, without probable cause, into the personal papers of the citizenry. Because of their long-held interests in privacy and in protecting citizens from government overreaching, *amici* are well-situated to provide this Court with additional insight into the issues presented here.

SUMMARY OF ARGUMENT

This case presents the important question of whether the Fourth Amendment allows the police to obtain a search warrant for *all* of a citizen's electronic communications, when the police have no probable cause to suspect that person of any crime and the only purpose of the search is to seize only the narrow and identifiable subset of those communications that relate to another person whom the police suspect committed a crime.

According to the Wisconsin Court of Appeals, *all* of a person's emails could be subject to seizure and search by law enforcement simply because that person has *received* some emails from an individual

suspected of a crime. This is a dangerous expansion of police power and inconsistent with this Court's clear message that the Fourth Amendment applies with full force to searches of digital records.

Last year, the Court recognized that the tremendous expansion in the amount of personal, private information that can be electronically stored has created growing opportunities for government intrusions on privacy. *See Riley v. California*, 134 S. Ct. 2473, 2488-89 (2014). Digital storage capabilities now "place vast quantities of personal information literally in the hands of individuals." *Id.* at 2485. Thus, the privacy interests in police searches of cell phones "dwarf" those of pre-digital searches incident to arrest, because a phone "not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id.* at 2491. Accordingly, the Court held that the government cannot lawfully conduct a warrantless search of a cell phone incident to arrest, absent other exigent circumstances. *Id.* at 2495.

The precise privacy concerns that animated the decision in *Riley* are equally at issue in the context of searches *with* a warrant. The Fourth Amendment guarantees that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Thus, the Fourth Amendment protects privacy by requiring that warrants be sufficiently

tethered to probable cause and meaningfully guide officers' discretion. Yet lower courts are increasingly confronted with overbroad warrants that seek *all* of a citizen's electronic information when there is only probable cause to search a specific and identifiable subset of that information. While many of those courts have faithfully applied the particularity requirement to such electronic searches, the Court of Appeals in this case did not, creating a split of authority that threatens the Fourth Amendment rights of citizens subject to electronic searches.

This case provides an excellent vehicle for the Court to address the degree to which the Fourth Amendment requires a search warrant for electronic information to be tailored to probable cause. Here, police had no probable cause to suspect Petitioner of any crime, and they obtained warrants to search her electronic communications solely in connection with their investigation of her co-worker, Tim Russell. As the Court of Appeals stated, the police sought to search Petitioner's accounts because those "accounts are believed to contain evidence in the form of emails sent to and received by Russell." Pet. App. 23. The police were interested in searching Petitioner's accounts "because emails deleted from Russell's Google account may have remained in [Petitioner's] accounts." Pet. App. 6.

Notwithstanding that narrow purpose, the warrants authorized law enforcement to rummage through *all* of Petitioner's electronic communications, regardless of whether they were sent to, received from, or even just mentioned Russell. Pet. App. 7-8.

The only limitation on the officers' discretion was the directive that they search for evidence of particular offenses—but they had no probable cause to believe that Petitioner committed those offenses, or that Petitioner had communicated with anyone who might have committed those offenses other than Russell.

The Wisconsin Court of Appeals nevertheless upheld the validity of the search warrants, and the Wisconsin Supreme Court denied the resulting appeal.[2] Its ruling conflicts with this Court's precedent and the approach taken by other lower courts in cases involving electronic searches, which have refused to authorize general rummaging through a person's electronic files when a more

---

[2] Although the Wisconsin Supreme Court denied the Petitioner's request to hear her case, recent developments indicate that at least one Justice was sufficiently concerned about the scope and the correctness of the Court of Appeals decision that, *sua sponte*, he moved the Supreme Court to reconsider its denial. As Justice Michael Gableman indicated in a letter to counsel dated June 30, 2015, he believed, after further review of the case, that the Court of Appeals' decision "eschews the Fourth Amendment's command and permits the government to rummage through Kelly Rindfleisch's digital files" when there was no probable cause to believe that "Rindfleisch's digital files had any evidence of any crime Rindfleisch might have committed." *See* Letter to Counsel from Hon. Michael J. Gabelman, Re: State v. Kelly M. Rindfleisch, 2013AP362-CR (June 30, 2015), *available at* http://cdn.wrn.com/wp-content/uploads/2015/06/201506301557-Rindfleisch.pdf. However, after learning that Petitioner had filed a petition for review with the U.S. Supreme Court, Justice Gableman withdrew his motion petition, believing that review in this Court was the better course of action. *Id.*

targeted search is possible. *See, e.g.*, *State v. Henderson*, 854 N.W.2d 616, 633 (Neb. 2014), *cert. denied*, No. 14-9519, 2015 WL 1942347 (U.S. June 15, 2015).; *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013); *United States v. Rosa*, 626 F.3d 56, 58, 62 (2d Cir. 2010; *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176-77 (9th Cir. 2010) (per curiam) (en banc); *United States v. Otero*, 563 F.3d 1127, 1132-33 (10th Cir. 2009).

At bottom, the Court of Appeals' ruling in this case gives the police *carte blanche* to search every electronic communication of any person who has any connection with a potential target in an investigation—even when the probable cause supporting that search is based solely on communications with one particular email address. This Court's review—either through a grant of *certiorari* or through summary reversal—is urgently needed.

ARGUMENT

I. The Court Should Grant *Certiorari* or Summarily Reverse the Decision Below Because of the Danger it Creates to Fourth Amendment Liberties.

Using key word searches, filters, and other simple techniques well-known to any litigator who has undertaken electronic discovery, electronic searches of digital files are regularly conducted in a manner calculated to yield all relevant information, while excluding irrelevant information. Such efforts

ensure the privacy of the person whose documents are being searched.

Yet under the Court of Appeals' ruling, so long as the government has reason to believe that a person may have received a single email relevant to a criminal investigation of a third party, the government is free to rummage through *all* of that person's electronic communications—without regard to whether the search could have been conducted more narrowly. Moreover, the ruling allows the government to do so without providing any notice to the person whose electronic communications are being seized. The decision therefore poses grave danger to Fourth Amendment liberties, and this Court should grant certiorari or summarily reverse.

A. The Particularity Requirement Mandates That a Search Warrant Be Narrowly Tailored to Probable Cause to Guard Against the Risks of General Warrants.

The Fourth Amendment's particularity requirement mandates that the government search no more broadly than probable cause can justify. The requirement was "the founding generation's response to the reviled 'general warrants' … of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 134 S. Ct. at 2494.

The particularity requirement prohibits the general warrant by requiring that a warrant limit the search to the "areas and things for which there is probable cause to search." *Maryland v. Garrison*,

480 U.S. 79, 84 (1987). By doing so, "the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Id.*; *see also Marron v. United States*, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."). The particularity requirement also ensures that the person whose possessions are subject to search and seizure has notice of that fact and of the limits of the officer's authority to search. *Cf. Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (explaining that notice to the person searched is a key function of the particularity requirement). A search conducted pursuant to a warrant that fails to conform to the particularity requirement is as unconstitutional under the Fourth Amendment as a warrantless search. *Id.* at 559-60.

Accordingly, in order to pass constitutional muster, warrants must "particularly describe[] evidence relating to a specific crime for which there is demonstrated probable cause." *Cassady v. Goering*, 567 F.3d 628, 636 (10th Cir. 2009) (quotation marks omitted); *see also Groh*, 540 U.S. at 560 (particularity requirement assures "that the Magistrate actually found probable cause to search for, and to seize, every item mentioned in the affidavit."). Thus, courts have upheld search

warrants authorizing the seizure of items like "marijuana and drug paraphernalia," *United States v. Young*, 420 F.3d 915, 917 (9th Cir. 2005), or "any and all firearms and ammunition," *United States v. Pulliam*, 748 F.3d 967, 972 (10th Cir. 2014), while more generic descriptions have been rejected. *See, e.g.*, *United States v. Morris*, 977 F.2d 677, 682 (1st Cir. 1992) ("[T]he catch-all phrase authorizing seizure of 'any other object in violation of the law' is impermissibly broad").

"The difference between a valid warrant and an overbroad warrant lies in whether the government could have phrased the warrant more specifically." *United States v. Le*, 173 F.3d 1258, 1275 (10th Cir. 1999); *see also, e.g.*, *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001) ("While a general order to explore and rummage is not permitted, the degree of specificity required is flexible and will vary depending on the crime involved and the types of items sought." (internal quotation marks omitted)); 2 Wayne R. LaFave, *Search & Seizure* § 4.6(a), at 767 (5th ed. 2012) ("[A]n otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based.").

Courts have long applied these principles when analyzing the constitutionality of warrants. For example, in *VonderAhe v. Howland*, 508 F.2d 364 (9th Cir. 1974), the Ninth Circuit found a warrant to be invalid for failing to restrict the search to the evidence the government knew it was looking for – yellow sheets and green cards of patient records kept

by a doctor. The government in that case "knew exactly what it needed and wanted and where the records were located." *Id.* at 370. The court determined that because the government knew with specificity the "'things' to be seized and the places to be searched," but used warrants that allowed a broader search, "the warrants as they were requested and issued were, for all practical purposes, 'general warrants'" and were therefore invalid. *Id.* at 366.

Similarly, in *Cassady*, the Tenth Circuit held that a warrant was invalid where it authorized a search of an entire farm for evidence including "all other evidence of criminal activity." 567 F.3d at 635 (quotation marks omitted). The court expressed concern that the warrant allowed "precisely the kind of rummaging through a person's belongings, in search of evidence of even previously unsuspected crimes or of no crime at all, that the fourth amendment proscribes." *Id.* (quoting *Voss v. Bergsgaard*, 774 F.2d 402, 405 (10th Cir. 1985)).

And nearly fifty years ago, this Court applied that same principle in holding that wiretaps were Fourth Amendment seizures. In invalidating a New York wiretapping law that allowed a wiretap of a particular person and telephone line upon an officer's oath that there is reasonable ground to believe evidence of crime could be obtained, the Court held that:

> [T]he statute's failure to describe with particularity the conversations sought gives the officer a roving commission to 'seize' any

> and all conversations. It is true that the statute requires the naming of 'the person or persons whose communications, conversations or discussions are to be overheard or recorded….' But this does no more than identify the person whose constitutionally protected area is to be invaded rather than 'particularly describing' the communications, conversations, or discussions to be seized. As with general warrants this leaves too much to the discretion of the officer executing the order.

Berger v. New York, 388 U.S. 41, 59 (1967) (alterations in original). The Court also emphasized that a wiretap warrant posed special Fourth Amendment dangers because it has "no requirement for notice as do conventional warrants." *Id.* at 60.[3]

As these decisions show, the particularity requirement serves a critical limiting function on warrants to ensure they comply with the Fourth Amendment.

---

[3] In enacting the Wiretap Act in 1968, Congress sought to address the privacy interests protected by the particularity requirement by providing that wiretaps "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." 18 U.S.C. § 2518(5).

B. The Decision of the Court of Appeals Eviscerates Fourth Amendment Protections Against Overbroad Electronic Search Warrants in Contravention of This Court's Decisions.

It follows naturally from this Court's particularity jurisprudence that when the government *can* narrow its search and seizure of electronic communications through the use of filters, key word searches, or other techniques, the particularity requirement mandates that it *must* do so. The decision below upends the limiting function of the particularity requirement by effectively exempting electronic searches from compliance with that requirement.

The Court of Appeals' decision therefore runs afoul of this Court's decisions recognizing the special importance of Fourth Amendment protections in the modern age of electronic communications. As this Court recognized in *Riley*, the sheer volume of personal information that can be stored and instantly accessed dwarfs what was imaginable just twenty years ago. While "[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so," *Riley*, 134 S. Ct. at 2489, the immense storage capacity of computers, cell phones, and electronic cloud storage now make it easy (and common) to have such information instantly accessible. A single email account may now have a decade or more of personal communications with spouses, parents and children;

confirmations for doctors appointments; receipts showing charitable or political donations; photos; contact information for friends, family, colleagues and acquaintances; bank statements; and news articles. These email accounts act as a digital diary of an individual's daily activities, struggles, health crises, romantic entanglements, political views, and personal contacts. Indeed, given the increasing prevalence of electronic data storage, the particularity requirement is even more essential today than it ever has been before.

In *Riley*, the Court recognized the high stakes involved when law enforcement officers conduct a search of private, electronically stored information. The "cache of sensitive personal information" that now can be digitally stored on a cell phone causes the search of a cell phone to "expose to the government far *more* than the most exhaustive search of a house." *Riley*, 134 S. Ct. at 2490, 2491. Accordingly, the Court held that such a search required a warrant. *Id.* at 2495. "Such a warrant ensures that the inferences to support a search are 'drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.'" *Id.* at 2482 (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)).

The protections that *Riley* deemed so vital will be undermined if magistrates are able to issue wide-ranging warrants for electronic information untethered to probable cause. Yet that is precisely the license given by the Court of Appeals here:

Police may obtain a warrant to search the entirety of an individual's electronic files and contacts, so long as there is reason to believe that a subset of certain, readily identifiable files might contain evidence of another's crime. Thus, the *entire* digital life of a person can be exposed, even where police have no probable cause to suspect that this person has engaged in any criminal wrongdoing, and even where police can easily tailor their search to those materials that they have probable cause to search. And moreover, police can conduct such a broad-ranging search without any notice to the person whose privacy interests are being invaded. The warrants in this case, after all, were issued to third party internet service providers, Google and Yahoo. In essence, the warrants approved by the Wisconsin Court of Appeals are the 21st-century version of the wiretap statute struck down by this Court in *Berger* nearly five decades ago.

C. The Decision by the Wisconsin Court of Appeals Conflicts with Decisions by Other Courts.

Numerous lower courts have applied the particularity requirements described above without any difficulty in the context of electronic searches. They have emphasized that warrants authorizing the search of electronic files must be tailored to the investigations' probable cause to ensure that they do not authorize the sorts of government intrusions that necessitated the Warrants Clause to begin with. The Second Circuit observed, "Like 18th Century 'papers,'" which the Founders were so committed to

protecting from general warrants, "computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion. If anything, even greater protection is warranted." *United States v. Ganias*, 755 F.3d 125, 135 (2d Cir. 2014), *reh'g en banc granted*, No. 12-240-CR, ___ F.3d ___, 2015 WL 3939426 (2d Cir. June 29, 2015).

The Tenth Circuit has held that a warrant was invalid for lack of particularity where it authorized the search of "any and all information and/or data" stored on a computer belonging to an individual suspected of committing mail fraud. *Otero*, 563 F.3d at 1132-33.

The Supreme Court of Nebraska held that a warrant to search a cell phone was invalid for allowing the search of "any and all information" held on the phone. *Henderson*, 854 N.W.2d at 633. The court emphasized that "a warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search." *Id.*

Similarly, the Second Circuit invalidated a warrant that permitted the search of, *inter alia*, "any written and/or printed and/or electronic stored notes or records which would tend to identify criminal conduct," because it "lacked the requisite specificity to allow for a tailored search of his electronic media." *Rosa*, 626 F.3d at 58, 62. The court explained, "The warrant was defective in failing to link the items to

be searched and seized to the suspected criminal activity," (the production and storage of child pornography) "and thereby lacked meaningful parameters on an otherwise limitless search of [the defendant's] electronic media." *Id.* at 62.

In *Comprehensive Drug Testing*, 621 F.3d at 1176, the Ninth Circuit expressed concern regarding precisely the sort of abuses that occurred in Petitioner's case. In that case, just as here, police had abused the warrant process to gobble up far more data and information than what it had probable cause to collect, and then attempted to use incriminating information found in the search that they had not had probable cause to seize. *Id.* at 1168.[4] The *Comprehensive Drug Testing* court acknowledged that law enforcement may sometimes legitimately "need to scoop up large quantities of data, and sift through it carefully." *Id.* at 1176. But the court also was firm that the "process of segregating electronic data that is siezeable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id.* at 1177. The court understood that without adequate safeguards, police would too easily be able to rummage through

[4] While the warrant at issue in *Comprehensive Drug testing* contained "significant restrictions" that were designed to ensure that "data beyond the scope of the warrant would not fall into the hands of the investigating agents," *id.*, law enforcement disregarded these safeguards and then attempted to use that data that exceeded the probable cause in the warrant to further its investigation, *id.* at 1171.

sensitive electronic files containing private details of individuals not suspected of any crime—exactly the sort of abuses that occurred in Petitioner's case. *See id.* ("Government intrusions into large private databases . . . have the potential to expose exceedingly sensitive information about countless individuals not implicated in any criminal activity, who might not even know that the information about them has been seized and thus can do nothing to protect their privacy.").

In short, where police have information that can be used to more particularly describe and target files to be seized through a search warrant, many lower courts have generally understood the particularity requirement to mandate that these limitations be included in the warrant.[5]

The Court of Appeals abandoned this essential requirement, and created a split with other lower courts, when it upheld the search and seizure of all

[5] Importantly, where more specific detail is *not* known to investigators, a more general search warrant may be permissible. *See, e.g.*, *United States v. Hanna*, 661 F.3d 271, 286 (6th Cir. 2011) (upholding more general warrant where the "government did not yet know all of the individuals or companies involved … [and] did not know where the materials were coming from, or the path these items took prior to reaching their final destination"); *United States v. Richards*, 659 F.3d 527, 541 (6th Cir. 2012) (upholding search of entire server for evidence of child pornography where "before the search, investigators did not know whether the server was shared or dedicated, and, if shared, whether any websites were related, whether users had access to the entire server, or how the directory was organized").

of Petitioner's personal communications. In this case, the affidavit in support of the search warrant application explained that the officers sought Petitioner's communications in connection with an investigation into Petitioner's co-worker, Tim Russell. Specifically, they sought emails between Petitioner and Russell that may have been deleted from Russell's own email accounts. The affidavit explained, "e-mails may not be found in the timrussellwi@gmail.com [account] because they have been deleted, but such e-mails may remain in [Petitioner's email account]." Pet. App. 6. The affidavit did not identify any probable cause to believe that Petitioner herself was suspected of any crime.

Despite this narrow basis for probable cause, the magistrate issued warrants authorizing the search of "[t]he contents of *all communications*" stored in Petitioner's Google and Yahoo email accounts, and with respect to the Google account, also allowed the search of "[a]ll address books, contact lists, friends[']lists, buddy lists, or any other similar compilations of personal contact information associated with the accounts." Pet. App. 7-8. (alterations in original). Approximately 16,000 documents of Petitioner's personal communications, generated over a 22-month period, were produced by Google and Yahoo in response to the warrants. Pet. App. 33, 49, 54.

There can be no doubt that the warrants *could have* been written with much more specificity and could have particularly described the electronic files the government had probably cause to look for. The

investigators knew precisely the type of evidence they were looking for, based on the probable cause that existed. And it would have been possible to segregate Petitioner's correspondence with Russell from the rest of her correspondence. Indeed, despite technological hurdles that sometimes arise when attempting to search electronic files for relevant evidence, courts have embraced the practice of using well-known discovery tools such as key word searches, "to"/"from" searches, or any of the other common tools, or even independent third parties to segregate those electronic files for which police have probable cause to seize, from those for which probable cause is lacking. *See In re Search Warrant*, 71 A.3d 1158, 1170 (Vt. 2012) ("Often the way to specify particular objects or spaces will not be by describing their physical coordinates but by describing how to locate them."); *see also id.* at 1180 (collecting cases where courts have approved use of third parties to assist in executing searches where the assistance will help limit the search to the relevant material).

Nevertheless, a divided panel of the Court of Appeals found no flaw in the warrants or the search and seizure of the entire body of Petitioner's electronic correspondence. A majority of the court rejected Petitioner's argument that the warrants at issue amounted to "general warrants" by failing to comply with the Fourth Amendment's particularity requirement. Pet. App. 23-24.

As an initial matter, the Court of Appeals relied on the fact that the "affidavit" identified the specific

email accounts among which the relevant electronic communications may have taken place. Pet. App. 24. That ruling flatly contradicts this Court's recent decision in *Groh*. There, the Court held that an affidavit cannot save an overly broad warrant. *Groh,* 540 U.S. at 557. "The Fourth Amendment by its terms requires particularity *in the warrant*, not in the supporting documents." *Id.* (emphasis added).[6] Thus, "[t]he fact that the *application* adequately described the 'things to be seized' does not save the *warrant* from its facial invalidity." *Id.* Consistent with this Court's holding in *Groh*, Federal Courts of Appeals have repeatedly invalidated warrants that lacked particularity – even where affidavits or other supporting documents provided greater detail. *See, e.g.*, *United States v. Tracey*, 597 F.3d 140, 149 (3d Cir. 2010); *Cassady*, 567 F.3d at 635; *United States v. McGrew*, 122 F.3d 847, 849-50 (9th Cir. 1997); *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992).

The Wisconsin Court of Appeals also held that the warrants complied with the particularity requirement because they "established, in no uncertain terms, that the State sought evidence of two particular crimes," Pet. App. 22, and identified

[6] The Court in *Groh* emphasized that the warrant at issue there "did not incorporate by reference the itemized list [of items to be seized] contained in the application." 540 U.S. at 554-55. Similarly, the warrants authorizing the collection of emails from Petitioners' personal accounts did not incorporate by reference the additional detail provided in the affidavits. *See* Pet. App. 50, 55.

"identified specific email accounts—four with Yahoo and two with Google—with which the warrants were concerned." *Id.* 24. But the logic of identifying the person whose communications were to be reviewed was precisely the logic this Court rejected in *Berger*. There, it held that identifying the person whose communications were to be overheard "does no more than identify the person whose constitutionally protected area is to be invaded rather than 'particularly describing' the communications, conversations, or discussions to be seized." *Berger*, 388 U.S. at 59.

Finally, the Wisconsin Court of Appeals also claimed to find support for the breadth of the electronic search warrants in the Ninth Circuit's decision in *United States v. Adjani*, 452 F.3d 1140 (9th Cir. 2006). *See* Pet. App. 20-23. But the Court of Appeals' reliance on *Adjani* was misplaced. *Adjani* in fact underscores the conflict created by the Wisconsin Court of Appeals' decision in this case.

In *Adjani*, a warrant authorized police to seize and search specific, defined types of records, documents and materials, as well as the computers and hard drives found in the home of an individual suspected of extortion. 452 F.3d at 1144. The warrant also allowed for the search of "all of the data contained in the computer equipment and storage devices" to find the specific types of records that were listed in the warrant. *Id.* One of the computers collected and ultimately searched belonged to a woman who lived with the suspect, who was not named as the target of the warrant. *Id.* at 1142. The

court upheld the legality of the search because "the government described the items to be searched and seized as particularly as could be reasonably expected given the nature of the crime and the evidence [the government] then possessed." *Id.* at 1149. But, importantly, the *Adjani* court emphasized that the warrant "instructed [the] agents to search for the documents reflecting communications with three individuals or other employees of a specific company." *Id.* at 1148.

These are precisely the kind of limiting instructions that the warrants in this case were lacking. Had the Court of Appeals in this case applied the approach set forth in *Adjani*, the case would have come out the other way. The fact that it did not, and the significance of the Constitutional violation here, warrant this Court's consideration.

CONCLUSION

The Court of Appeals' decision sets a dangerous precedent for police searches of electronic information. Under the rule it adopted, anyone who has received an email from an individual suspected of a crime is at risk of having *all* of their communications collected and reviewed by law enforcement. Law enforcement officials then will be free to review masses of information while they pick and choose the communications that they wish to use to build any case—even for crimes or activities wholly unrelated to the probable cause supporting the warrant. This is precisely the sort of general rummaging that the warrants clause is designed to prevent.

This rule is inconsistent with other lower courts' decisions and contrary to the requirements of the Fourth Amendment. Only this Court's intervention can ensure that the "privacies of life," *Riley*, 134 S. Ct. at 2485, in citizens' personal email accounts are shielded from an unjustified, exploratory rummaging by police.

For the foregoing reasons, the Court should grant the Petitioner's petition for writ of certiorari or summarily reverse.

Respectfully submitted,

ILYA SHAPIRO
CATO INSTITUTE
1000 Mass. Ave. NW
Washington, DC 20001
(202) 842-0200
ishapiro@cato.org

LINDSAY C. HARRISON
Counsel of Record
JULIA M. CARPENTER
MATTHEW E. PRICE
ELIZABETH C. BULLOCK
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
lharrison@jenner.com

Counsel for Amici Curiae

July 13, 2015