No. _____

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

PETITION FOR WRIT OF CERTIORARI

TODD P. GRAVES
Counsel of Record
EDWARD D. GREIM
LUCINDA H. LUETKEMEYER
GRAVES GARRETT LLC
1100 Main Street, Suite 2700
Kansas City, MO 64105
(816) 256-3181
tgraves@gravesgarrett.com
edgreim@gravesgarrett.com
lluetkemeyer@gravesgarrett.com

FRANKLYN M. GIMBEL
KATHRYN A. KEPPEL
GIMBEL, REILLY, GUERIN & BROWN LLP
Two Plaza East, Suite 1170
330 East Kilbourn Avenue
Milwaukee, WI 53202
(414) 271-1440
fgimbel@grgblaw.com
kkeppel@grgblaw.com

QUESTION PRESENTED

Does the Fourth Amendment permit a search warrant authorizing the unfettered seizure of all of an individual's emails from her internet service provider for a specified period of time, without limiting the seizure to communications containing evidence of a crime?

PARTIES TO THE PROCEEDING

Petitioner Kelly M. Rindfleisch was the defendant in the circuit court for Milwaukee County and the appellant in the Wisconsin Court of Appeals. Respondent the State of Wisconsin was the plaintiff in the circuit court for Milwaukee Country and the respondent in the Wisconsin Court of Appeals. The Wisconsin State Public Defender filed a brief as amicus curiae before the Wisconsin Supreme Court in support of Rindfleisch's Petition for Review of the Court of Appeals' decision.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

PARTIES TO THE PROCEEDING ii

TABLE OF CONTENTS iii

TABLE OF AUTHORITIES vi

PETITION FOR A WRIT OF CERTIORARI 1

OPINIONS BELOW 3

JURISDICTION 4

CONSTITUTIONAL AND STATUTORY PROVISIONS 4

STATEMENT OF THE CASE 4

REASONS FOR GRANTING THE PETITION 11

I. The Warrants for the Search and Seizure of Petitioner's Entire Email Accounts for Almost Two Years Were "General Warrants" in Violation of the Fourth Amendment 13

A. The Fourth Amendment Prohibits General Warrants 13

B. The Unique Nature of Digital Searches and Seizures Necessitates Heightened Sensitivity to the Fourth Amendment's Particularity Requirement 16

C. The Warrants Authorizing Seizure of All of Petitioner's Electronic Communications, Rather Than Those Containing Evidence of a Crime, Violate the Fourth Amendment's Prohibition on General Searches 21

TABLE OF CONTENTS – Continued

Page

II. This Court Should Grant Review to Address the Important and Pressing Issue of Fourth Amendment Law Raised by the Decision Below 25

A. Warrants for Digital Data That Appear Particular on Their Face Risk Becoming General in Practice 25

B. As Evidenced by Court Decisions and Scholarly Debate, Courts Differ on the Application of the Fourth Amendment to the Search and Seizure of Stored Electronic Communications 28

C. The Court Should Grant Review to Resolve the Application of Dated Fourth Amendment Law to Search Warrants for Stored Electronic Communications 33

CONCLUSION 36

APPENDIX

State v. Rindfleisch, 2014 WI App 121, 359 Wis. 2d 147 .....App. 1

Wisconsin Circuit Court Judgment of Conviction, Nov. 27, 2012.....App. 37

Wisconsin Circuit Court Order, Sept. 14, 2012 .....App. 39

Wisconsin Circuit Court Decision (Excerpt).....App. 41

Wisconsin Circuit Court Search Warrant, Oct. 20, 2010.....App. 49

TABLE OF CONTENTS – Continued

Page

Wisconsin Circuit Court Search Warrant, Oct. 20, 2010.....App. 49

Wisconsin Supreme Court Denial of Review, Mar. 16, 2015.....App. 59

Constitutional Provisions and Statutes .....App. 61

TABLE OF AUTHORITIES

Page

CASES

Andresen v. Maryland, 427 U.S. 463 (1976).....15, 28

Ashcroft v. al-Kidd, 131 S. Ct. 2074 (2011).....13

Bartnicki v. Vopper, 532 U.S. 514 (2001).....18

City of Ontario v. Quon, 560 U.S. 746 (2010).....18

Coolidge v. New Hampshire, 403 U.S. 443 (1971).....13, 15

Dalia v. United States, 441 U.S. 238 (1979).....14

Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997).....15

Ex Parte Jackson, 96 U.S. 727 (1877).....17

In re Cellular Telephones, 2014 WL 7793690 (D. Kan. Dec. 30, 2014).....28, 32

In re Search Warrant, 193 Vt. 51, 71 A.3d 1158 (2012).....30, 31

In re U.S.'s Application For A Search Warrant To Seize & Search Elec. Devices From Edward Cunnius, 770 F. Supp. 2d 1138 (W.D. Wash. 2011).....26, 32, 34

In the Matter of Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-9191-DJW Target Email Address, Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917.....30

In the Matter of the Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1 (D.D.C. 2013).....32

TABLE OF AUTHORITIES – Continued

Page

In the Matter of the Search of Premises Known as Nextel Cellular Telephone, 2014 WL 2898262 (D. Kan. June 26, 2014).....31

Kyllo v. United States, 533 U.S. 27 (2001).....20

Lopez v. United States, 373 U.S. 427 (1963).....20

Marron v. United States, 275 U.S. 192 (1927).....16

Maryland v. Garrison, 480 U.S. 79 (1987).....13

Matter of Black iPhone 4, 27 F. Supp. 3d 74 (D.D.C. 2014).....33

Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d (D.D.C. 2014).....30

Riley v. California, 573 U.S. ___, 134 S. Ct. 2473 (2014).....*passim*

State v. Meyer, 216 Wis. 2d 729 (1998).....23

State ex rel. Newspapers, Inc. v. Circuit Court for Milwaukee Cnty., 65 Wis. 2d 66, 221 N.W.2d 894 (1974).....5

Steagald v. United States, 451 U.S. 204 (1981).....14

United States v. Ali, 870 F. Supp. 2d 10 (D.D.C. 2012).....18

United States v. Bickle, 2011 WL 3798225 (D. Nev. July 21, 2011).....32

United States v. Bowen, 689 F. Supp. 2d 675 (S.D.N.Y. 2010).....32

TABLE OF AUTHORITIES – Continued

Page

United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009) 30

United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) 25

United States v. Cioffi, 668 F. Supp. 2d 385 (E.D.N.Y. 2009) 23, 26

United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) .....*passim*

United States v. Forrester, 512 F.3d 500 (9th Cir. 2008) 18

United States v. Galpin, 720 F.3d 436 (2d Cir. 2013) 13, 19, 27

United States v. Ganias, 755 F.3d 125 (2d Cir. 2014) 14

United States v. Hill, 459 F.3d 966 (9th Cir. 2006) 12

United States v. Jacobsen, 466 U.S. 109 (1984) 17

United States v. Jones, 132 S. Ct. 945 (2012) 19

United States v. Leary, 846 F.2d 592 (10th Cir. 1988) 22

United States v. Mann, 592 F.3d 779 (7th Cir. 2010) 29, 31

United States v. Maxwell, 45 M.J. 406 (U.S. Ct. Armed Forces 1996) 18

United States v. Otero, 563 F.3d 1127 (10th Cir. 2009) 26

TABLE OF AUTHORITIES – Continued

Page

United States v. Stabile, 633 F.3d 219 (3d Cir. 2011) 29

United States v. Stubbs, 873 F.2d 210 (9th Cir. 1989) 22

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982) 15, 25

United States v. Taylor, 764 F. Supp. 2d 230 (D. Me. 2011) 32

United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297 (1972) 14, 15

United States v. Van Leeuwen, 397 U.S. 249 (1970) 17

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) 17, 18, 20

United States v. Williams, 592 F.3d 511 (4th Cir. 2010) 30

United States ex rel. Milwaukee Social Democratic Publishing Co. v. Burleson, 255 U.S. 407 (1921) 17

Wilson v. Moreau, 440 F. Supp. 2d 81 (D.R.I. 2006) 17

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. IV .....*passim*

U.S. Const. amend. XIV 4, 8, 9

TABLE OF AUTHORITIES – Continued

Page

STATUTES AND RULES

28 U.S.C. § 1257(a) 4

Wis. Stat. § 968.26 5

Wis. Stat. § 946.12(3) 4, 8, 9

BOOKS AND ARTICLES

Athul K. Acharya, *Semantic Searches*, Duke L. J. 393 (November 2013) 19

Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored Email*, 2008 U. Chi. Legal F. 121 (2008) 20

DOJ Computer Evidence Manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 15

Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored Email Surveillance*, 90 Neb. L. Rev. 971 (2012) 20, 28

Stephen Guzzi, *Digital Searches and the Fourth Amendment: The Interplay Between the Plain View Doctrine and Search-Protocol Warrant Restrictions*, 49 Am. Crim. L. Rev. 301 (Winter 2012) 23

Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005 (April 2010) 25

TABLE OF AUTHORITIES – Continued

Page

Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241 (2010) 29

Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005) 11

Kaitlin R. O'Leary, *What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine*, 46 Suffolk U. L. Rev. 211 (2013) 26

Raphael Winick, *Searches and Seizures of Computers and Computer Data*, Harvard J.L. & Tech. 75 (1994) 25

PETITION FOR A WRIT OF CERTIORARI

Petitioner Kelly M. Rindfleisch respectfully petitions for a writ of certiorari to review the judgment of the Wisconsin Court of Appeals, District I, in Case No. 2013AP362-CR.

This case involves a significant question of law: whether the Fourth Amendment's breadth and particularity provisions protect non-target witnesses from warrants that allow investigators to seize and search every email they sent, received, or deleted over an extended period. Such warrants – typically directed to emails stored on the server of an internet service provider such as Google or Yahoo – are increasingly common and easy to obtain. They often fail to specify the relevant criminal conduct, and mandate no protocol (like key word searches) for finding relevant evidence. Instead, they allow limitless browsing. The split decision of the Wisconsin Court of Appeals approved just such a search. In so doing, it nullified Fourth Amendment protections for citizens' digital and electronic data. Not just in Wisconsin, but in many other state and federal courts that find themselves nearing the bottom of a decades-long slippery slope, the state may now seize a citizen's entire email account, search it in secret, and retain all of the seized email for future perusal.

In such meandering digital searches, the evidence sought comprises a mere fraction of a witness's email file. The rest of the witness's emails are nonetheless perused, however, and as a result often find

their way into evidence under the "plain view" doctrine. In such cases, one could reasonably question how the warrant, search, and seizure differs at all from the general searches that the Fourth Amendment's particularity requirement was designed to avert. State and federal courts have grappled with the issue for years, but little progress has been made, and in the absence of initial guidance from this Court, none is imminent. There is a reason that lower courts are permanently stuck at square one: they cannot agree that a problem of constitutional gravity even exists. A recent decision, however, has set the stage for this Court to enter this arena and provide the requisite initial guidance. In *Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473, 2490 (2014), the Court held that law enforcement officers may not search cell phones incident to a warrantless arrest without first obtaining a warrant. Critically, the Court recognized that electronic and digital information is quantitatively and qualitatively different from physical records. This is precisely the distinction that the Court of Appeals rejected in this case when it firmly took the side of lower courts that refuse to recognize the constitutional danger arising from the convergence of non-particular email warrants and the plain view doctrine.

Ms. Rindfleisch's case, then, poses a logical follow-up question to *Riley*. Now that a warrant is required to search digital data on a cell phone, for example, must it also avoid overbreadth, and must it also have the requisite particularity? And, given the inherent

differences between physical and computer searches and seizures, should courts allow seizures beyond the scope of a warrant under the plain view doctrine, which could result in massive over-seizing of data and turn specific warrants into general ones?

Drawing on its holding in *Riley*, this Court should recognize the principle that digital and electronic search warrants like the one directed to Ms. Rindfleisch's archive of personal communications violate the Fourth Amendment's breadth and particularity protections. By so doing, this Court will prune an errant branch of the law – exemplified by the Court of Appeals' refusal to recognize the application of the Fourth Amendment. This pruning will trigger new growth elsewhere, and it will bear fruit: lower court decisions will now be free to explore particularity requirements for warrants in specific contexts, and – as in other areas – legislatures may well exercise their prerogative to enact statutory protocols to protect witnesses and aid law enforcement.

OPINIONS BELOW

The opinion of the Wisconsin Court of Appeals (App. 1) can be found at 2014 WI App 121, 359 Wis. 2d 147, 857 N.W.2d 456. The order of the Supreme Court of Wisconsin denying review (App. 59) is unpublished. The relevant trial court proceedings and order (App. 39, 41) are unpublished.

JURISDICTION

The Wisconsin Court of Appeals grounded its decision in the federal constitution. App. 2. The Supreme Court of Wisconsin denied review on March 16, 2015. App. 59. This Court has jurisdiction pursuant to 28 U.S.C. § 1257(a).

CONSTITUTIONAL AND STATUTORY PROVISIONS

The United States Constitution's Fourth and Fourteenth Amendments and Wisconsin Statutes § 946.12(3) are reproduced in the appendix at App. 61.

STATEMENT OF THE CASE

In early 2010, Petitioner Kelly Rindfleisch was hired as a policy advisor for Scott Walker, then serving as Milwaukee County Executive. She was soon promoted to Deputy Chief of Staff. Rindfleisch was issued a laptop computer and a state email account. Rindfleisch also had a personal laptop computer and cell phone for which she created and owned personal email accounts with internet service providers (ISPs) Yahoo and Gmail.

In late 2010, as part of a "John Doe" investigation[1] into Walker staffers at the County Executive's office, law enforcement officials delved into communications among Walker's County Executive staff, his gubernatorial campaign staff, and the campaign staff for lieutenant governor candidate Brett Davis. The State sought evidence that Tim Russell, Walker's Chief of Staff at Milwaukee County, had committed various alleged crimes. In hopes of finding evidence of Russell's crimes, the State applied for and received search warrants for the personal Google and Yahoo email accounts of Rindfleisch. App. 5, 22.

The warrants ordered Google and Yahoo to produce *all* communications stored on Rindfleisch's email accounts, including all emails, whether sent or received or stored in "deleted" status, for a 22-month period. App. 49, 54.

The search warrant directed to Yahoo demands production of:

> (a) The contents of all communications stored in the Yahoo accounts for the subscriber(s) identified above, including all emails stored in the account, whether sent from or received in the account as well as e-mails held in a "Deleted" status;
>
> (b) All records or other information regarding the identification of the accounts, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account statuses, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
>
> (c) All records pertaining to communications between Yahoo, Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

App. 49. The search warrant directed to Gmail demands production of:

> (a) The contents of all communications stored in the Gmail accounts for the subscriber(s) identified above, including all emails stored in the account, whether sent from or received in the account as well as e-mails held in a "Deleted" status;

[1] Wisconsin's "John Doe" statute provides for secret criminal investigatory proceedings supervised by a judge, serving in a quasi-prosecutorial capacity, in lieu of a grand jury. Wis. Stat. § 968.26; *State ex rel. Newspapers, Inc. v. Circuit Court for Milwaukee Cnty.*, 65 Wis. 2d 66, 70-71, 221 N.W.2d 894, 896 (1974).

(b) All address books, contact lists, friends lists, buddy lists, or any other similar compilations of personal contact information associated with the accounts;

(c) All records or other information regarding the identification of the accounts, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account statuses, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

(d) All records pertaining to communications between Gmail (Google) and any person regarding the accounts, including contacts with support services and records of actions taken.

App. 54.

In all, Google and Yahoo produced approximately 16,000 documents of Rindfleisch's personal communications. App. 33. The warrants did not direct Google and Yahoo to search those 16,000 documents for evidence of Russell's alleged crimes. They instead assigned that task to law enforcement. App. 49, 54.

It is undisputed that neither the search warrants nor the affidavits supporting those warrants implicated Rindfleisch in any improper behavior. App. 20, 34. Instead, the affidavits of the state's investigator asserted that evidence of *Russell's* misconduct would be found in Rindfleisch's email accounts. App. 5-6. According to the state, Rindfleisch's alleged culpability became "apparent" only after prosecutors received the warrant return. App. 34.

The communications were provided to investigators without any independent review or filtering agent to ensure protection of Rindfleisch's privacy interests. App. 33-34. Prosecutors relied on the "plain view" exception to justify their discovery of emails that revealed that Rindfleisch sent and was copied on emails related to campaign activities during normal business hours. *Id.* Even though the state acknowledged it lacked any belief that Rindfleisch was involved in any improper activity when the warrants were issued, the state relied on the seized email communications to charge her. *Id.*

The state filed a criminal complaint charging Rindfleisch with four counts of felony misconduct in public office, in violation of Wis. Stat. § 946.12(3). Rindfleisch moved to suppress all evidence obtained via the search warrants on grounds that the warrants lacked the requisite particularity, were overly broad, and were general warrants, eviscerating her rights under the Fourth and Fourteenth Amendments to the United States Constitution and correlative provisions of the Wisconsin Constitution. The circuit court

denied the motion, finding that the search warrants were not constitutionally defective and the search was not in "flagrant disregard for the limitations" of the warrant. App. 14, 39, 46.

Rindfleisch petitioned the Wisconsin Court of Appeals for leave to appeal the circuit court's decision, but that petition was denied. App. 14. Thereafter, following extensive plea negotiations, Rindfleisch entered and the circuit court accepted a plea of guilty to one count of misconduct in public office, a Class I felony, in violation of Wis. Stat. § 946.12(3). *Id.*

Rindfleisch appealed the judgment of conviction, arguing again that the sweeping nature of the warrants for all of her emails in the 22-month period rendered them "general warrants," violating her rights under the Fourth and Fourteenth Amendments. App. 16.

The Wisconsin Court of Appeals, in a 2-1 decision, affirmed her conviction, holding that the warrants at issue did not violate the Fourth Amendment's particularity requirements. App. 2. In reaching its decision, the majority concluded that there is no difference between traditional searches of file cabinets and drawers and searches of digital data:

> [A] search warrant for a filing cabinet, located in a particular place, which contains a year's worth of correspondence between, or relating to, two particular individuals, would normally be searched where the filing cabinet is located by the officers executing the warrant. Likewise, many documents in that filing cabinet would have nothing to do with either of those individuals. The only way the officer could distinguish between what relates to either of those individuals and what does not, is to look through all of the documents in the filing cabinet. Law enforcement officers have long had to separate the documents as to which seizure was authorized from the other documents. So far, as we have been able to discover, that necessity has not turned an otherwise valid warrant into a "general" warrant. We see no constitutional imperative that would change the result simply because the object of the search is electronic data from a specific electronic file, for a reasonably specific period of time, in the custody of a specific ISP.

App. 27-28.

The majority repeatedly chastised Rindfleisch for failing to prove which of the 16,000 emails produced and searched exceeded the scope of the warrants. App. 23, 24, 28. The court further emphasized that the internet service providers stated in writing "that they provided *only* what was required by the warrant, and they removed electronic data beyond the scope of the warrant." App. 28.

Judge Ralph Adam Fine dissented. App. 30. Judge Fine explained that the warrants at issue, which authorized the seizure of *all* email in Rindfleisch's accounts regardless of sender, recipient, or subject matter, were unconstitutionally overbroad. According to Judge Fine, the warrants violated the Fourth

Amendment because they failed to "set out probable cause that Rindfleisch had done anything wrong (as the Fourth Amendment requires)" and failed to "describe any place where any evidence that she had done anything wrong could be found (as the Fourth Amendment also requires)." App. 32. Judge Fine found that the majority's opinion "legitimizes a general warrant and nullifies our Constitution." App. 36.

Rindfleisch sought discretionary review in the Wisconsin Supreme Court. As is pertinent here, she renewed her argument that the warrants violated the Fourth Amendment. The Wisconsin Supreme Court denied review without comment. App. 59-60.

REASONS FOR GRANTING THE PETITION

One of the most pressing challenges in criminal justice is the preservation of constitutional protections for citizens' electronic communications and records – particularly the application of the Fourth Amendment protection from unreasonable search and seizure. As one scholar has noted, computers have become the equivalent of "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more." *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005).

By directing the seizure of *all* of Rindfleisch's personal email for almost two years and failing to particularly describe the emails to be seized, or even limit the seizure to emails related to a crime, the warrants allowed law enforcement to "seize the haystack to look for the needle" – here, evidence of another person's misconduct. *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006). The language of the warrants used to seize and search Rindfleisch's entire email accounts was overbroad and insufficiently particular to satisfy the Fourth Amendment. By this decision, Wisconsin courts have ignored the grave invasion of privacy that results when searches for digital and electronic data proceed unfettered by any reasonable limitation to ensure the protection of a citizen's rights.

The Court of Appeals' treatment of Rindfleisch's challenge exemplifies one side of the growing division among courts regarding the application of the Fourth Amendment to the search and seizure of stored electronic communications. The Court should grant certiorari to determine whether a warrant directing an internet service provider to give investigating officers an entire email account so they may search every email for evidence of a crime is a "general warrant" in violation of the Fourth Amendment.

I. The Warrants for the Search and Seizure of Petitioner's Entire Email Accounts for Almost Two Years Were "General Warrants" in Violation of the Fourth Amendment.

A. The Fourth Amendment Prohibits General Warrants.

The Fourth Amendment requires 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. These restrictions are "the founding generation's response to the reviled 'general warrants' and 'writs of assistance' 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 manifest purpose of the Fourth Amendment's particularity requirement is to combat the Framers' chief evil: general searches. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). *See also Ashcroft v. al-Kidd,* 131 S. Ct. 2074, 2084 (2011) ("The Fourth Amendment was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown."); *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (" . . . the specific evil is the 'general warrant' abhorred by the colonists. . . ."); *United States v. Galpin,* 720 F.3d 436, 445 (2d Cir. 2013).

A general search "le[aves] to the discretion of the executing officials the decision as to which persons

should be arrested and which places should be searched . . . [and] provide[s] no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home." *Steagald v. United States*, 451 U.S. 204, 220 (1981). "The Framers abhorred [general searches], believing that 'papers are often the dearest property a man can have' and that permitting the Government to 'sweep away all papers whatsoever,' without any legal justification, 'would destroy all the comforts of society.'" *United States v. Ganias*, 755 F.3d 125, 134 (2d Cir. 2014).

This Court has stated: "Though the Fourth Amendment speaks broadly of 'unreasonable searches and seizures,' the definition of 'reasonableness' turns, at least in part, on the more specific commands of the warrant clause." *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 315 (1972). The Warrant Clause has three requirements: authorization by a neutral and detached magistrate; a demonstration of probable cause that evidence will be found in a particular location; and a particularized description of the things to be seized and the place to be searched. *See Dalia v. United States*, 441 U.S. 238, 255 (1979). The Warrant Clause has been

> a valued part of our constitutional law for decades, and it has determined the result in scores and scores of cases in courts all over this country. It is not an inconvenience to be somehow 'weighed' against the claims of police efficiency. It is, or should be, an

> important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly over-zealous executive officers' who are a party of any system of law enforcement.

Id., 407 U.S. at 315-16 (quoting *Coolidge*, 403 U.S. at 481). The particularity requirement serves to ensure that government agents "conduct narrow seizures that attempt to 'minimize[ ] unwarranted intrusions upon privacy.'" DOJ Computer Evidence Manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, at 70 (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)).

A warrant must provide the officer conducting the search with sufficiently precise language to allow him to determine which items are properly subject to seizure and which items are irrelevant. *See Davis v. Gracey,* 111 F.3d 1472, 1478-79 (10th Cir. 1997) ("We ask two questions: did the warrant tell the officers how to separate the items subject to seizure from irrelevant items, and were the objects seized within the category described in the warrant?"); *accord United States v. Tamura,* 694 F.2d 591, 595 (9th Cir. 1982) (stating that a request to search must be accompanied by "sufficiently specific guidelines for identifying the documents sought . . . [to be] followed by the officers conducting the search.").

Thus, "[t]he 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." *Marron v. United States,* 275 U.S. 192, 196 (1927). In other words, "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Id.*

B. The Unique Nature of Digital Searches and Seizures Necessitates Heightened Sensitivity to the Fourth Amendment's Particularity Requirement.

In today's age of stored electronic communications, the protections afforded by the Fourth Amendment's particularity requirement are more important than ever. At the time most Fourth Amendment cases were decided, individuals could protect their personal letters, photographs or other documents by simply destroying them, resting easy knowing that those documents never would see the light of day. With electronic and digital data, however, nothing is ever truly destroyed. Forensic experts can obtain documents from computer servers, and even documents never transferred to anyone can be recovered from hard drives. "Electronic storage and transmission of data is no longer a peculiarity or a luxury of the very rich; it's a way of life." *See*, *e.g.*, *United States v. Comprehensive Drug Testing, Inc.* (*CDT III*), 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam).

The Fourth Amendment explicitly protects private "papers" from unreasonable searches and seizures. U.S. Const. amend. IV. This Court has recognized

that the Framers intended to protect the privacy of written communications as much as a journal slid into a drawer. *See United States v. Jacobsen*, 466 U.S. 109, 114-15 (1984) (holding that there is a legitimate expectation of privacy in letters and other sealed packages); *Ex Parte Jackson*, 96 U.S. 727, 733 (1877) ("Whilst in the mail, [letters] can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.").

A person's digital papers, such as email, should enjoy at least as much constitutional protection as a letter delivered by the post office.[2] Several courts have recognized that emails and other electronic records are entitled to the same Fourth Amendment protections as older forms of communication. *See*, *e.g.*, *United States v. Warshak,* 631 F.3d 266, 285-86 (6th Cir. 2010) ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."); *Wilson v. Moreau*, 440 F. Supp. 2d 81, 108 (D.R.I. 2006) (finding reasonable expectation of privacy in content of Yahoo email

[2] Postal mail has always been protected by the Fourth Amendment. *See United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970); *Ex Parte Jackson*, 96 U.S. 727, 733 (1877). As Justice Holmes noted, "The use of the mails is almost as much a part of free speech as the right to use our tongues." *United States ex rel. Milwaukee Social Democratic Publishing Co. v. Burleson*, 255 U.S. 407, 427 (1921) (Holmes, J., dissenting).

account); *United States v. Maxwell*, 45 M.J. 406, 418 (U.S. Ct. Armed Forces 1996) (" . . . an expectation of privacy exists in e-mail transmissions made on the AOL service. . . ."); *see also Bartnicki v. Vopper*, 532 U.S. 514, 541 (2001) (Rehnquist, C.J., dissenting) ("Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business email. . . .").

The Sixth Circuit endorsed this conclusion in *Warshak*, reasoning that email "is the technological scion of tangible mail" and that it would "defy common sense to afford emails lesser Fourth Amendment protection." 631 F.3d at 285-86 (citing *City of Ontario v. Quon*, 560 U.S. 746, 762-63 (2010) ("implying that 'a search of [an individual's] personal e-mail account' would be just as intrusive as 'a wiretap on his home phone line'"). *See also United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) ("holding that '[t]he privacy interests in [mail and email] are identical'")).

Because "computers and email accounts often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize," the particularity requirement of the Fourth Amendment has taken on renewed importance in the digital age. *United States v. Ali*, 870 F. Supp. 2d 10, 39 (D.D.C. 2012) (internal quotation marks and citations omitted); *accord*

Galpin, 720 F.3d at 447 (when "the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance."). Indeed, today, the search of a digital device "would typically expose to the government far *more* than the most exhaustive search of a house." *Riley*, 134 S. Ct. at 2491. This is equally true for a search conducted on a Google or Yahoo account. Records obtained from Google and other email service providers allow the government to identify where a user was when she logged in to the account and provide an immense amount of information about actions the user took in any given day. *Cf. United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (describing the Fourth Amendment concerns presented by GPS information, which "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

When investigating officers obtain a warrant to seize a person's entire email account on the grounds that they have probable cause to believe that it contains evidence of another person's crime, they cannot know what the emails contain without opening and viewing them. So, one-by-one, they open thousands of email messages, click on the embedded links, examine the attachments and expose a vast archive of a person's life (here, 22 months' worth) to "plain view." *See* Athul K. Acharya, *Semantic Searches*, Duke L. J. 393, 404-405 (November 2013). If the person's sent, received or deleted email include evidence incriminating her or others, the government may seize it without a warrant and use it to prosecute her or anyone else with whom she communicated. *See* Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored Email Surveillance*, 90 Neb. L. Rev. 971, 989, 1011 (2012); Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored Email*, 2008 U. Chi. Legal F. 121, 138 (2008).

The Court has cautioned that new technologies should not be allowed to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34; *see also Warshak*, 631 F.3d at 285 ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.").[3] The Court again recognized this problem in *Riley*, reasoning that Fourth Amendment privacy protection must account for this new technological reality. There, in holding that cell phones may not be searched under the search-incident-to-arrest warrant exception, the court noted that modern cell phones – just like cloud-based email – are capable of

[3] As Justice Scalia has noted, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001); *see also Lopez v. United States*, 373 U.S. 427, 459 (1963) (Brennan, J., dissenting) ("The Constitution would be an utterly impractical instrument of contemporary government if it were deemed to reach only problems familiar to the technology of the eighteenth century. . . .").

storing a vast amount of personal information and thus deserve the highest privacy protections. *Riley*, 134 S. Ct. at 2491.

What the Court wrote about cell phones in *Riley* applies equally to email: modern email contains "[t]he sum of an individual's private life," including "a record of all his communications," and materials such as prescriptions and bank statements. *Id.* at 2489. The concerns animating *Riley* apply equally here and strongly support the position that law enforcement access to electronic communications requires a sufficiently specific warrant that comports with the Fourth Amendment.

C. The Warrants Authorizing Seizure of All of Petitioner's Electronic Communications, Rather Than Those Containing Evidence of a Crime, Violate the Fourth Amendment's Prohibition on General Searches.

The warrants and affidavits in this case generally described categories of documents to be seized without any particularity other than a time frame and a relationship to Rindfleisch's email addresses. They authorized the seizure of each and every email during the time period, regardless of its nature. The warrants left it to law enforcement officers to sift through Rindfleisch's personal, private communications to determine which of those communications actually related to their case. As such, they failed to establish probable cause that all of the information

the state sought constituted evidence of any crime or evidence, and if so, what. *See United States v. Stubbs*, 873 F.2d 210 (9th Cir. 1989) (warrant describing generic categories of documents without any effort to specifically describe the items which the officers could have seized under a probable cause standard). Such warrants lack particularity because "'[b]y listing every type of record that could conceivably be found in an office, the warrant effectively authorized the inspectors to cart away anything they found on the premises.'" *United States v. Leary*, 846 F.2d 592, 602-03 (10th Cir. 1988).

Ignoring the nature and reality of modern electronic communications, the majority of the Wisconsin Court of Appeals held that the "seize then search" of an entire email account is just like a "search then seize" of incriminating letters in a filing cabinet. App. 27.

In so holding, the majority ignored the fact that digital searches and seizures, by their nature, uniquely implicate the "plain view" doctrine, raising questions about the general searches the Fourth Amendment's particularity requirement was designed to avert. As Judge Fine noted in his dissent, the warrants at issue are indistinguishable from "general warrants" because they authorized the seizure of *all* email in Rindfleisch's accounts regardless of sender, recipient, or subject matter.

Had the warrants for Rindfleish's email accounts complied with the Fourth Amendment's particularization requirement and delineated the emails to be

seized, such as those related to a crime, they would not have authorized a wholesale rummaging through Rindfleisch's personal email. The absence of such a limitation was a significant factor in suppressing the fruits of a warrant for an entire email account in *United States v. Cioffi*, 668 F. Supp. 2d 385 (E.D.N.Y. 2009). In that case, the court held that the warrant was unconstitutionally overbroad because it "did not, on its face, limit the items to be seized from [the person's] personal email account to emails containing evidence of the crimes charged in the indictment at all." *Id.* at 396. Like the warrant in *Cioffi*, the warrants here contain no limitation to the emails to be seized, other than the time period, and therefore are impermissible general warrants in violation of the Fourth Amendment.

The majority below repeatedly chastised Rindfleisch for failing to prove which of the 16,000 emails produced and searched exceeded the scope of the warrants, but in doing so missed the point. Whether the language of the warrant satisfies requisite constitutional requirements is a question of law, not fact. *See State v. Meyer*, 216 Wis. 2d 729 (1998). Furthermore, the majority mistakenly characterized Rindfleisch's arguments about the scope of the warrant as "rhetorical salvos," ignoring that "the cardinal danger of general warrants looms in the application of the plain view doctrine to the digital realm." *See* Stephen Guzzi, *Digital Searches and the Fourth Amendment: The Interplay Between the Plain View Doctrine and*

Search-Protocol Warrant Restrictions, 49 Am. Crim. L. Rev. 301, 335 (Winter 2012).

Under the Wisconsin Court of Appeals' decision, *any* document, once emailed to another person, is fair game for review by law enforcement officers, no matter that law enforcement has no probable cause, not even a reasonable suspicion, that the individual whose records are being seized has committed a crime. This rationale is no different from the mindset of colonial revenue officers that led to the creation of the Fourth Amendment. Like the revenue officers and others who invaded colonial homes looking for evidence despite having no reason to believe the homeowner was guilty of any offense, Wisconsin has authorized law enforcement to enter the "cyber-homes" of Rindfleisch and other citizens not suspected of criminal activity to seize all electronic communications and browse for evidence of someone else's wrongdoing.

It is antithetical to the Fourth Amendment to allow law enforcement officers to seize and then search all of an individual's private, personal electronic and digital files without limitation, without notice, and without cause. The result here is exactly what the Founding Fathers sought to prohibit. As the dissent explained, the majority's holding "legitimizes a general warrant and nullifies our Constitution." *See* App. 36.

II. This Court Should Grant Review to Address the Important and Pressing Issue of Fourth Amendment Law Raised by the Decision Below.

A. Warrants for Digital Data That Appear Particular on Their Face Risk Becoming General in Practice.

The court below wrongly concluded that there is no difference between traditional searches of file cabinets and drawers and searches of digital data – a conclusion that has been sharply disputed by other courts and commentators. *Compare* App. 27 *with United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) ("Relying on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'") (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data,* Harvard J.L. & Tech. 75, 104 (1994); *see also Tamura,* 694 F.2d at 595-96 (unlike file cabinets, computers and electronic storage systems often contain "intermingled documents"); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1007 (April 2010) (physical space differs from Internet space, and these differences require courts to find new ways to maintain the function of the Fourth Amendment in an online environment).

The danger of general warrants looms when officers browsing digital data are allowed to wander off course under the plain view doctrine. Digital searches

capture vast quantities of data, including innocent and personal information with no relevance to the asserted crimes. Moreover, such searches provide a limitless portal to other devices, data and individuals, rendering a warrant authorizing seizure of "all" email communications limitless. *In re U.S.'s Application For A Search Warrant To Seize & Search Elec. Devices From Edward Cunnius*, 770 F. Supp. 2d 1138, 1144-45 (W.D. Wash. 2011). The ability to store and intermingle a huge array of personal information in one place, such as in an email account, "increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important." *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009).

An email account likely contains not only emails possibly relevant to an investigation, but also emails and files "the government has no probable cause to search and seize." *See CDT III*, 621 F.3d at 1176; *Cioffi*, 668 F. Supp. 2d at 391. If the government must open every electronic file on a computer, or every email in an account, to know its contents, then everything the government chooses to open will come into plain view. Kaitlin R. O'Leary, *What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine*, 46 Suffolk U. L. Rev. 211, 224 (2013) (allowing officers to open every file exposes all contents to plain view thereby creating a "general warrant" in violation of the

Fourth Amendment). As Judge Fine wrote in his dissent in the court below:

> The danger in this type of case is palpable:
>
> > [B]ecause there is currently no way to ascertain the content of a file without opening it and because files containing evidence of a crime may be intermingled with millions of innocuous files, "[b]y necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there." Once the government has obtained authorization to search the hard drive, the government may claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant. There is, thus, "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches.

App. 32 (quoting *Galpin*, 720 F.3d at 447 (quoted sources omitted)).

Greater vigilance by judicial officers is required to strike "the right balance between the government's interest in law enforcement and the right of

individuals to be free from unreasonable searches and seizures." Friess, 90 Neb. L. Rev. at 987 (citing *CDT III*, 621 F.3d at 1177). Officers must ensure searches and seizures of stored emails occur in a manner minimizing unwarranted intrusions upon privacy. *Id*. (citing *Andresen*, 427 U.S. at 482 n.11).

B. As Evidenced by Court Decisions and Scholarly Debate, Courts Differ on the Application of the Fourth Amendment to the Search and Seizure of Stored Electronic Communications.

As technology continues to evolve, it becomes increasingly difficult to apply the Fourth Amendment's particularity requirement to search warrants for electronically stored information. "The absence of guidance from the Supreme Court and lack of agreement among lower courts have resulted in conflicting approaches to these types of warrants around the country. [T]hese various approaches have given rise to some confusion on the issue." *In re Cellular Telephones*, 2014 WL 7793690, at *3 (D. Kan. Dec. 30, 2014).

There is a national debate on the permissibility and usefulness of placing conditions on search warrants for electronically stored information, and on the application of the plain view doctrine to digital searches. Federal and state courts, now including Wisconsin, have set out contradictory visions of the appropriate scope of a digital search and the applicability of the plain view doctrine to digital searches. *See*, *e.g.*, *CDT III*, 621 F.3d at 1178-80 (Kozinski, C.J.,

concurring); *United States v. Stabile*, 633 F.3d 219, 240-41 & n.16 (3d Cir. 2011); *United States v. Mann*, 592 F.3d 779, 785-86 (7th Cir. 2010); Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241, 1260-71 (2010).

One federal court "urged the government to adopt a procedure that would allow it to obtain the information it legitimately needs for criminal investigations while respecting the Fourth Amendment" and listed courts' various approaches of:

1. Asking the electronic communications service provider to provide specific limited information such as emails or faxes containing certain key words or emails sent to/from certain recipients;

2. Appointing a special master with authority to hire an independent vendor to use computerized search techniques to review the information for relevance and privilege;

3. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant;

4. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases; and

5. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.

Matter of the Search of Info. Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 7-8 (D.D.C. 2014).[4]

Some courts apply the plain view doctrine to search warrants for electronically stored information. The Fourth, Seventh, and Tenth Circuits, for example, all appear to maintain some version of the plain view doctrine in the context of digital searches, but take different approaches in confining the scope of such searches. The Fourth and Tenth Circuits use the "file cabinet" analogy. *See United States v. Williams*, 592 F.3d 511, 522-23 (4th Cir. 2010) (applying an expansive filing-cabinet approach, which provides a broad application of plain view), *and United States v. Burgess*, 576 F.3d 1078, 1092-94 (10th Cir. 2009) (same). The Seventh Circuit examines the search protocol used in light of the search authorized by the

[4] *See In the Matter of Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-9191-DJW Target Email Address,* Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917, at *10 (items 1-2); *CDT III,* 621 F.3d at 1180 (Kozinski, J., concurring) (items 3-5); *see also In re Search Warrant,* 193 Vt. 51, 71 A.3d 1158, 1186 (2012) (upholding nine *ex ante* restrictions on a search warrant for electronic data but holding that the issuing officer could not prevent the government from relying on the plain view doctrine).

warrant. *See Mann*, 592 F.3d at 785-86 (finding incremental fact-based adjudication most appropriate, preserving plain view as a possibility).

Other courts have concluded that because computer searches bring so much information to officers' attention, the plain view doctrine must be limited. *See, e.g., In re Search Warrant*, 193 Vt. 51, 71 A.3d 1158 (2012) (holding that a judicial official who issued a computer search warrant could require that the search be conducted by third parties behind a "firewall," and that the search team provide to investigators only information relevant to the offense that gave rise to the search warrant). Similarly, the Ninth Circuit has approved a warrant that prescribed procedures for ensuring that electronic data was segregated by independent law enforcement computer personnel so that only the information described in the warrant was turned over to the investigating officers. *CDT III*, 621 F.3d at 1176-77 (noting that "over-seizing is an inherent part of the electronic search process"). The Ninth Circuit has suggested that magistrate judges issuing search warrants should take steps to limit the government's access to data for which it has no probable cause, such as requiring an on-site assessment of the feasibility of seizing only responsive data, requiring data segregation to be done by someone other than the case agent, and perhaps limiting the government's plain view rights. *Id.*

Some district courts ask magistrate judges to require warrants to specifically outline the protocols to be used in a digital evidence search. *See In the Matter*

of the Search of Premises Known as Nextel Cellular Telephone, 2014 WL 2898262, at *7 (D. Kan. June 26, 2014) (listing very specific search protocols that would satisfy the Fourth Amendment); *In re Cellular Telephones*, 2014 WL 7793690, at *8. Other courts require use of a filter team. *See Cunnius*, 770 F. Supp. 2d at 1144 (denying an application for search warrant where the government refused to "conduct its search of the digital devices utilizing a filter team and foreswear[ ] reliance on the plain view doctrine").[5]

Some courts issuing warrants for electronic information have included "secondary orders" imposing "minimization procedures" concerning the Government's handling and retention of material disclosed by third-party custodians of electronic information. These courts require that records outside the scope of the search warrants be "returned" to the custodian or, in the case of copies, "destroyed." *See In the Matter of the Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.,* 21 F. Supp. 3d 1, 9-10 (D.D.C. 2013); *see also*

[5] Other courts disagree, holding that the "Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching." *United States v. Taylor,* 764 F. Supp. 2d 230, 237 (D. Me. 2011); *accord United States v. Bickle*, 2011 WL 3798225, at *20 (D. Nev. July 21, 2011); *United States v. Bowen,* 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010).

Matter of Black iPhone 4, 27 F. Supp. 3d 74, 80 (D.D.C. 2014) (denying application and stating that in any future application the "government must specify what will occur" with "data that is seized by the government and is outside the scope of the warrant").

A grant of review in this case will allow this Court to resolve these differing approaches and settle the growing confusion regarding government access to and use of digital and electronic communications sought in a search warrant.

C. The Court Should Grant Review to Resolve the Application of Dated Fourth Amendment Law to Search Warrants for Stored Electronic Communications.

Technological advances allow covert government intrusion into the private lives of citizens never contemplated by the Framers of the Constitution. Technology provides opportunities for investigators to invade privacy without prior notice, and without leaving any clues that they slipped into a citizen's "cyber-house." Concerns over the constitutionality of government monitoring of the personal lives of its citizens are exacerbated when the government authorizes a search warrant for *all* communications stored in a citizen's email account, without limiting the seizure to communications containing evidence of a crime. Such broad warrants allow investigators to read private communications between a citizen and his or her lawyer,

priest, rabbi, physician, psychiatrist or spouse. They allow access to private medical information intended to be shared only with family and close friends. In balancing the government's need to investigate with the constitutional rights of citizens, warrants authorizing search and seizure of digital information must include constitutional safeguards to protect civil rights. *See Cunnius*, 770 F. Supp. 2d at 1151-52.

The decision of Wisconsin Court of Appeals that there is no difference between traditional searches of file cabinets and searches of email accounts and other digital data ignores these concerns and the realities of evolving technology. As this Court confirmed in *Riley*, courts must consider what is and is not a "reasonable" search and seizure in the context of the quantitative and qualitative distinctions between papers in a file cabinet and electronically-stored digital data.

Federal and state courts have set out contradictory visions of the appropriate scope of digital searches. Only some of those approaches properly balance the government's investigatory interests with the rights of individuals to be free from unreasonable searches and seizures. As technology continues to advance, challenges to the seizure and search of digital records repeatedly will be presented to federal and state courts. Decades-old Fourth Amendment jurisprudence is no longer viable for assessing warrants issued for digital information.

This case offers this Court an ideal vehicle to draw on its holding in *Riley* to recognize the principle that digital and electronic search warrants like the one directed to Rindfleisch's archive of personal communications violate the Fourth Amendment. By so doing, this Court will prune an errant branch of the law – exemplified by the Court of Appeals' refusal to recognize the application of the Fourth Amendment's particularity requirement in the digital context. Such a ruling would provide much needed clarity to law enforcement, courts, and legislators, resulting in search warrants for electronic information that are reasonable and sufficiently particular under the Fourth Amendment. Lower courts would then be free to explore particularity requirements for warrants in specific contexts, and – as in other areas – legislatures may well exercise their prerogative to enact statutory protocols to protect witnesses and aid law enforcement.

The orderly administration of justice cries out for this Court to grant certiorari to analyze the Fourth Amendment's application to such records and to resolve courts' contradictory visions of the appropriate scope of a digital search.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

TODD P. GRAVES
Counsel of Record
EDWARD D. GREIM
LUCINDA H. LUETKEMEYER
GRAVES GARRETT LLC
1100 Main Street, Suite 2700
Kansas City, MO 64105
(816) 256-3181
tgraves@gravesgarrett.com
edgreim@gravesgarrett.com
lluetkemeyer@gravesgarrett.com

FRANKLYN M. GIMBEL
KATHRYN A. KEPPEL
GIMBEL, REILLY, GUERIN & BROWN LLP
Two Plaza East, Suite 1170
330 East Kilbourn Avenue
Milwaukee, WI 53202
(414) 271-1440
fgimbel@grgblaw.com
kkeppel@grgblaw.com

Counsel for Petitioner

COURT OF APPEALS
DECISION
DATED AND FILED

November 12, 2014

Diane M. Fremgen
Clerk of Court of Appeals

Appeal No. 2013AP362-CR **Cir. Ct. No. 2012CF438**

STATE OF WISCONSIN

IN COURT OF APPEALS
DISTRICT I

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

v.

KELLY M. RINDFLEISCH,

DEFENDANT-APPELLANT.

APPEAL from a judgment of the circuit court for Milwaukee County: DAVID A. HANSHER, Judge. *Affirmed*.

Before Curley, P.J., Fine and Kessler, JJ.

¶1 KESSLER. J. At issue in this appeal is whether the circuit court erred in denying Kelly M. Rindfleisch's motion to suppress all evidence resulting from a search warrant ordering Internet Service Providers (ISPs) Google and Yahoo to produce emails from Rindfleisch's email accounts with them from

January 1, 2009, until October 10, 2010, together with the account ownership identifying data. Rindfleisch claims the warrants lacked sufficient particularity and thus were "general warrants" in violation of her Fourth Amendment rights. We affirm.

BACKGROUND

¶2 Rindfleisch was charged with four counts of misconduct in public office, in violation of WIS. STAT. § 946.12(3) (2009-10),[1] based on a complaint alleging that she engaged in partisan campaign activities, including political fundraising, during working hours while she was simultaneously a Milwaukee County employee working for then-County Executive Scott Walker. The criminal complaint alleged that during her County work hours, Rindfleisch campaigned for Walker's 2010 gubernatorial campaign, along with the campaign for Lieutenant Governor Candidate Bret Davis.

---

[1] WISCONSIN STAT. § 946.12 (2009-10) provides: "Any public officer or public employee who does any of the following is guilty of a Class I felony: . . . (3) [w]hether by act of commission or omission, in the officer's or employee's capacity as such officer or employee exercises a discretionary power in a manner inconsistent with the duties of the officer's or employee's office or employment or the rights of others and with intent to obtain a dishonest advantage for the officer or employee or another."

All references to the Wisconsin Statutes are to the 2011-12 version unless otherwise noted.

¶3 The complaint states that Rindfleisch was hired by the County Executive's Chief of Staff, Tim Russell, as a policy advisor for the County Executive in early 2010. Rindfleisch was promoted to Deputy Chief of Staff in March 2010. As a Milwaukee County employee, Rindfleisch was issued a laptop and a County email account. According to the complaint, Rindfleisch used a "non-County issued, personal laptop computer and a non-County, private wireless Internet connection supplied by Tim Russell," to work on "projects assigned to her by Russell." Rindfleisch also had two personal email accounts: rellyk_us@yahoo.com and kmrindfleisch@gmail.com. Information found in the emails subject to the warrants showed that both of Rindfleisch's personal email accounts were used for political purposes during County work hours.

¶4 On August 11, 2010, Milwaukee County District Attorney Chief Investigator David Budde submitted an affidavit requesting multiple search warrants relating to political activity conducted by Darlene Wink, the Constituent Services Coordinator for Walker. The affidavit incorporated by reference both an affidavit dated May 14, 2010, in support of a petition to enlarge the scope of the John Doe proceedings[2] investigating various potentially prohibited

[2] A John Doe proceeding is described in, and authorized by, WIS. STAT. § 968.26. It authorizes a judge, at the request of a district attorney, to conduct a secret court proceeding to investigate whether a crime has been committed and if so, by whom.

(Continued on following page)

activities conducted by Walker's aides or appointees during his time as Milwaukee County Executive, and an affidavit dated July 1, 2010, "in support of a Search Warrant for the Yahoo Mail accounts of Darlene Wink." According to the August 11, 2010 affidavit, both of the incorporated affidavits tended to establish that Wink conducted partisan political activity while engaged in her official position as an employee within the Office of Milwaukee County.[3]

¶5 Shortly thereafter, the John Doe proceedings expanded to include Russell.[4] On August 20, 2010,

The judge has the power to subpoena witnesses, take testimony, and issue subpoenas and warrants.

The John Doe proceedings were initiated by prosecutors in 2010 to investigate potentially illegal campaign activities conducted by Walker aides, appointees, and employees during his time as Milwaukee County Executive. The May 14, 2010 request to enlarge the scope of the John Doe proceedings was related to "blog posting activity by Darlene Wink as 'rpmcvp' while serving as an employee in the Office of the County Executive."

[3] In May 2012, Darlene Wink resigned from her position shortly after a *Milwaukee Journal Sentinel* reporter "requested Wink's payroll records . . . to determine whether she was doing political work on county time."

[4] Russell was ultimately charged with three counts of theft by embezzlement, contrary to WIS. STAT. § 943.20(1)(b), after then-County Executive Walker designated a nonprofit corporation controlled by Russell to manage the "Operation Freedom" funds used for an annual veterans event run by the Milwaukee County Executive's office. Russell ultimately pled guilty to one of the theft-by-embezzlement counts. His conviction is being appealed in case No. 2014AP451-CR.

Budde submitted another affidavit, "principally to search and seize records and information in the form of digital evidence contained on computer workstations issued by Milwaukee County for Tim Russell's use." The affidavit did not refer to, or implicate, Rindfleisch. However, an exhibit to the affidavit included an email from Russell to Rindfleisch, including the email chain to which Russell's email related. The chain included various emails discussing political matters. The email addresses in the chain included Russell's email address, "JillB@scottwalker.org," Rindfleisch's Milwaukee County email account and her Google email account.[5]

¶6 Two months later, on October 20, 2010, Budde submitted another affidavit supporting a search warrant application to require emails between January 1, 2009, and October 20, 2010, from Rindfleisch's Google and Yahoo accounts, and from the email accounts for Russell, Brian Pierick, and "ScottForGov." The affidavit explained that Budde believed the email accounts would contain evidence of

[5] It is apparent from the record in this case that the State necessarily followed numerous email trails in the John Doe proceedings to determine the extent of statutorily prohibited political and fundraising activity occurring in government offices and/or on government time. While the record before us suggests that approximately sixteen thousand emails from the identified Rindfleisch accounts were produced by the ISPs in response to the warrants, that is hardly surprising in view of the significant number of people receiving copies and the twenty-two months involved.

Russell's misconduct in public office because emails deleted from Russell's Google account may have remained in Rindfleisch's accounts. Budde explained why Rindfleisch's email accounts would probably contain evidence of Russell's misconduct:

> While e-mail accounts will often contain many e-mails dating back over months or even years, it is entirely probable that . . . over time a user can delete 'without a trace' some e-mails held in accounts that are hosted by a provider of electronic communications services. That is to say that e-mails may not be found in the timrussellwi@gmail.com because they have been deleted, but such e-mails may remain in the Rindfleisch [account].
>
> A review of the e-mail threads in this investigation suggest that a number of potentially relevant e-mails have been deleted from the timrussellwi[@]gmail inbox. Evidence from the Rindfleisch accounts will either tend to establish the completeness of the e-mail evidence thus far collected, or it will provide additional evidence of otherwise deleted e-mails. In either event, the evidence from these e-mail accounts will be relevant and valuable.

¶7 The warrants issued to Google and Yahoo on October 20, 2010,[6] were substantially similar. Both

[6] The affidavit indicates that the time period involved in the request, namely January 1, 2009, "to the present," i.e. October

(Continued on following page)

contained information identifying the statutory authority of the investigation (the John Doe proceeding), and the identifying email account information for the ISPs. Both warrants required:

> **RECORDS TO BE PRODUCED**: For the time period of January 1, 2009, to the present, this warrant applies to information associated with the account identified as . . . stored at premises owned, maintained, controlled, or operated by [the ISP at their respective headquarters address]. This warrant requires, **ON OR BEFORE NOVEMBER 22, 2010** the production of:
>
> a. The contents of all communications stored in the [ISP] accounts for the subscriber(s) identified above, including all emails stored in the account, whether sent from or received in the account as well as e-mails held in a "Deleted" status;
>
> b. All records or other information regarding the identification of the accounts, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account statuses, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
>
> c. All records pertaining to communications between [the ISP] and any person regarding the accounts, including contacts with support services and records of action taken.

20, 2010, was "reasonably related to the current campaign season for the Office of the Governor." Rindfleisch has not argued that the time period involved was unreasonable.

¶8 The warrant issued to Google additionally included the following production request:

> All address books, contact lists, friends['] lists, buddy lists, or any other similar compilations of personal contact information associated with the accounts;

¶9 Both warrants requested the ISPs to search for evidence of the specific crimes of misconduct in public office and political solicitation involving public officials and employees. The warrants state that the search was to be "for the following evidence of crime":

> For the time period of January 1, 2009 to the present, all records relating to Misconduct in Public Office and Political Solicitation involving Public Officials and Employees, violations of §§ 946.12, 11.36 and 11.61 of the Wisconsin Statutes, including information relating to the financial or other benefit provided to any private and/or political cause or

organization either effected using Milwaukee County facilities or effected during periods of normal county work hours or both.

The terms "records" and "information" include all items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage.

Which objects constitute evidence of the commission of a crime, to wit;

DESCRIBE CRIME OR CRIMES:

(1) Misconduct in Public Office; and

(2) Political Solicitation involving Public Officials and Employees committed in violation of sections 946.12, 11.36[7] and 11.61[8] of the Wisconsin Statutes.

---

[7] WISCONSIN STAT. §11.36 provides:

Political solicitation involving public officials and employees restricted.

(1) No person may solicit or receive from any state officer or employee or from any officer or employee of the University of Wisconsin Hospitals and Clinics Authority any contribution or service for any political purpose while the officer or employee is engaged in his or her official duties, except that an elected state official may solicit and receive services not constituting a contribution from a state officer or employee or an officer or employee of the University of Wisconsin Hospitals and Clinics Authority with respect to a referendum only. Agreement to perform services authorized under this subsection may not be a condition of employment for any such officer or employee.

(Continued on following page)

Both warrants allowed the records to be delivered to the District Attorney's office.

¶10 The ISPs complied with the warrants by sending the District Attorney: (1) subscriber identifying information for the provided email address(es); (2) session timestamps and originating IP addresses

---

(2) No person may solicit or receive from any officer or employee of a political subdivision of this state any contribution or service for any political purpose during established hours of employment or while the officer or employee is engaged in his or her official duties.

(3) Every person who has charge or control in a building, office or room occupied for any purpose by this state, by any political subdivision thereof or by the University of Wisconsin Hospitals and Clinics Authority shall prohibit the entry of any person into that building, office or room for the purpose of making or receiving a contribution.

(4) No person may enter or remain in any building, office or room occupied for any purpose by the state, by any political subdivision thereof or by the University of Wisconsin Hospitals and Clinics Authority or send or direct a letter or other notice thereto for the purpose of requesting or collecting a contribution.

(5) In this section, "political purpose" includes an act done for the purpose of influencing the election or nomination for election of a person to national office, and "contribution" includes an act done for that purpose.

(6) This section does not apply to response by a legal custodian or subordinate of the custodian to a request to locate, reproduce or inspect a record under s. 19.35, if the request is processed in the same manner as the custodian or subordinate responds to other requests to locate, reproduce or inspect a record under s. 19.35.

[8] WISCONSIN STAT. §11.61 describes the criminal penalties applied to, and entities responsible for prosecution of, political solicitation involving government employees.

for logins for the dates requested in the warrant; and (3) CDs containing the emails and contacts lists available to the ISP for the dates requested.[9]

¶11 On October 28, 2010, Google responded to the warrant stating: "To the extent any document provided herein contains information exceeding the scope of your request, protected from disclosure or otherwise not subject to production, if at all, we have redacted such information or removed such data fields." At oral argument, counsel for Rindfleisch stated that on November 1, 2010, the State asked to have the John Doe proceedings expanded to include Rindfleisch. Others were also included in the expanded proceedings. The State requested a search warrant for Rindfleisch's Milwaukee dwelling in West Allis and her Columbia County property. Counsel advised at oral argument that these warrants were executed, with Rindfleisch present, and her personal computer(s) seized. Her counsel also stated that the computer warrants were not being challenged and are not part of this appeal.

¶12 Yahoo responded on November 19, 2010, swearing in an affidavit: "Pursuant to the Federal Stored Communications Act, 18 USC §§ 2701 *et. Seq.,* we have redacted information, including removing

[9] Rindfleisch has not objected to the account ownership information, times and dates of email transmissions, etc. required by the warrants. Consequently, we limit our discussion to her objection to production of the text content of the emails.

certain data fields, that exceeds the scope of this request, is protected from disclosure or is otherwise not subject to production."

¶13 On January 26, 2012, Rindfleisch was charged with four counts of misconduct in public office. The specific dates[10] of the four alleged offenses were all in the Spring of 2010 (prior to the date of the warrants), and all were supported by electronic evidence. The criminal complaint includes copies of several emails between Rindfleisch and Russell, using her Google and Yahoo accounts. It also identifies multiple chat transcripts between Rindfleisch and other campaign aides. These electronic communications, along with other information in the complaint, indicate that Rindfleisch intentionally engaged in partisan political campaign activities[11] during her Milwaukee County work time.

¶14 Rindfleisch filed a motion to suppress all evidence obtained as a result of the search warrants issued to Yahoo and Google. Rindfleisch argued that the warrants "purportedly permitted by . . . section 968.375, *Stats.,* eviscerates her privacy rights under

[10] The dates of the alleged offenses were April 3, 2010, April 16, 2010, May 3, 2010, and May 4, 2010.

[11] According to a chat transcript referenced in the complaint, Rindfleisch told a friend that her private laptop was on a "separate system," making it possible for her to discuss campaign activities at work. In that same chat transcript, she also told her friend that "half of what I'm doing is policy for the campaign."

the Fourth and Fourteenth amendments and correlative provisions under the Wisconsin Constitution . . . [and] may well run afoul of Rindfleisch's other constitutional protections, including her rights under the First and Sixth Amendments and HIPPA (*sic*) laws."[12] The focus of Rindfleisch's suppression argument to the circuit court was that: (1) the warrants failed to identify the objects to be seized with requisite particularity; and (2) WIS. STAT. § 968.375 is unconstitutional as applied to her case. Rindfleisch argued in her brief supporting her motion that "[t]he warrants required an unknown employee of the ISPs to produce all of their records, and then left it to law enforcement officers to sift through [her] personal, private communications to determine which of those communications actually related to the case. . . . The ISPs complied with the warrants. Law enforcement officers then had *carte blanche* to rummage through [her] personal electronic communications."

¶15 After briefing and a hearing, the circuit court orally denied Rindfleisch's motion, finding:

> [T]he warrants authorized the search of specific e-mail accounts for a specific time period for specific crimes which evidenced campaign activity by government employees. Even if the warrants were overbroad, I find the

[12] Rindfleisch does not develop arguments on appeal which rely on the Fourteenth, First, or Sixth Amendments of the United States constitution, nor on HIPAA laws. Thus those claims are abandoned.

> items are within the scope of the warrants – or the items within the scope of the warrants should not be suppressed because the search is not conducted in, quote, flagrant disregard for the limitations, end of quote, of the warrant.
>
> Generally items seized within the scope of a warrant need not be suppressed simply because other items outside the scope of the warrant were also seized, unless the entire search was conducted in a flagrant disregard for the limitations of the warrant.

¶16 Rindfleisch subsequently pled guilty to one count of misconduct in public office; the State dismissed the remaining three counts. The circuit court withheld sentence and placed Rindfleisch on probation for a period of three years, imposed a six-month period of confinement with Huber release privileges in the House of Correction, and ordered her to pay costs and surcharges. This appeal is limited by WIS. STAT. § 971.31(10) to the circuit court's denial of Rindfleisch's motion to suppress the evidence obtained from Google and Yahoo.

DISCUSSION

A. Standard of Review.

¶17 "On review of a motion to suppress, [an appellate] court employs a two-step analysis." ***State v. Dubose,*** 2005 WI 126, ¶16, 285 Wis. 2d 143, 699 N.W.2d 582. "First, we review the circuit court's

findings of fact. We will uphold these findings unless they are against the great weight and clear preponderance of the evidence." ***Id.*** We "'will uphold findings of evidentiary or historical fact unless they are clearly erroneous.'" ***Id.*** (citation omitted). "Next, we must review independently the application of relevant constitutional principles to those facts. Such a review presents a question of law, which we review de novo, but with the benefit of [the analysis] of the circuit court." ***Id.*** (internal citation omitted).

B. Motions to Suppress Evidence.

¶18 When a party moves to suppress evidence based on an alleged Fourth Amendment violation, the proponent of the motion has the burden of establishing that his Fourth Amendment rights were violated. ***State v. Bruski,*** 2007 WI 25, ¶20, 299 Wis. 2d 177, 727 N.W.2d 503. The burden of offering evidence at a suppression hearing has been helpfully described by Wayne R. LaFave in *Search and Seizure: A Treatise On The Fourth Amendment*:

> At the hearing on the motion to suppress, who has the burden of proof with respect to the matters at issue? To understand the full significance of this inquiry, it is first necessary to recall that the term "burden of proof" actually encompasses two separate burdens. One burden is that of producing evidence, sometimes called the "burden of evidence" or the "burden of going forward." If the party who has the burden of producing evidence does not meet that burden, the consequence is an adverse ruling on the matter at issue. The other burden is the burden of persuasion, which becomes crucial only if the parties have sustained their respective burdens of producing evidence and only when all the evidence has been introduced.

See 6 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment,* § 11.2(b) (4th ed. 2004) (footnotes omitted).

C. The Warrant Clause and General Warrants.

¶19 Rindfleisch argues that her Fourth Amendment rights have been violated because the warrants here are "general warrants," which "lack the level of particularity required to pass constitutional muster." Specifically, Rindfleisch asserts that:

> the warrants required unknown employees of the ISPs to produce *all of their records,* and then left it to law enforcement officers to sift through Rindfleisch's personal, private communications to determine which of those communications actually related to their case.

(Emphasis added.)

¶20 The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.*

(Emphasis added.) It is upon this last clause that Rindfleisch bases her entire argument. Specifically, Rindfleisch contends that the warrants at issue lacked sufficient particularity and were unconstitutional general warrants.

¶21 The United States Supreme Court, in ***Steagald v. United States,*** 451 U.S. 204 (1981), explained the background and definition of a general warrant:

> The Fourth Amendment was intended partly to protect against the abuses of the general warrants that had occurred in England and the writs of assistance used in the Colonies. *The general warrant specified only an offense* – typically seditious libel – and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched. Similarly, *the writs of assistance* used in the Colonies *noted only the object of the search* – any uncustomed goods – and thus left customs officials completely free to search any place where they believed such goods might be. *The central objectionable feature of both warrants was that they provided no judicial check on the determination of the executing officials* that the evidence available justified an intrusion into any particular home.

See ***id.*** at 220 (internal citations omitted, emphasis added).

D. The Warrants at Issue did not Violate the Fourth Amendment's Particularity Requirements.

¶22 Typically, when officers exceed the scope of a search warrant, the remedy is to suppress only items seized outside the scope of the warrant. ***State v. Petrone,*** 161 Wis. 2d 530, 548, 468 N.W.2d 676 (1991), *overruled on other grounds by* ***State v. Greve,*** 2004 WI 69, ¶31 n.7, 272 Wis. 2d 444, 681 N.W.2d 479. However, if the search is conducted in "flagrant disregard" of the limitations in the warrant, all items seized – even items within the scope of the warrant – are suppressed. ***Petrone,*** 161 Wis. 2d at 548. When a search is conducted with flagrant disregard for the limitations found in the warrant, the Fourth Amendment's "particularity requirement is undermined and a valid warrant is transformed into a general warrant thereby requiring suppression of all evidence seized under that warrant." ***United States v. Medlin,*** 842 F.2d 1194, 1199 (10th Cir. 1988).

¶23 "The United States Supreme Court has interpreted the Warrant Clause to be precise and clear, and as requiring only three things: (1) prior authorization by a neutral, detached [judicial officer]; (2) a demonstration upon oath or affirmation that there is probable cause to believe that evidence sought will aid in a particular conviction for a

particular offense; and (3) a particularized description of the place to be searched and items to be seized." ***State v. Sveum***, 2010 WI 92, ¶20, 328 Wis. 2d 369, 787 N.W.2d 317 (citations and quotation marks omitted).

¶24 Keeping in mind the Supreme Court's definition of a general warrant and its interpretation of the Warrant Clause, we measure the warrants at issue against each requirement provided by the Warrant Clause.

1. Prior Authorization by a Neutral, Detached Judicial Officer.

¶25 The warrants were signed on October 3, 2010 by an experienced jurist, Reserve Judge Neal Nettesheim.[13]

2. Demonstration by an Oath or Affirmation that there is probable cause to believe that the evidence seized will lead to a particular conviction of a particular offense.

¶26 David E. Budde, the Chief Investigator assisting the John Doe Judge, swore to an affidavit in support of both the Google warrant and the Yahoo

[13] Judge Nettesheim served as a Circuit Court Judge from 1975 to 1984. He served as a Court of Appeals Judge from 1984 until his retirement in 2007. He was appointed by the Wisconsin Supreme Court to preside over the John Doe proceeding in which he issued the warrants in question.

warrant. His affidavit contained numerous pages of detailed information, along with multiple exhibits.

¶27 The affidavit stated the warrants request related "to violations of Wisconsin Statutes § 964.12 [sic], Misconduct in Public Office, by Milwaukee County employee Timothy Russell of the Department of Health and Human Services (and formally of the Milwaukee County Executive's Office)." The affidavit explained that "county desktop computers used by Tim Russell were seized pursuant to search warrants" in this investigation, and forensic examination of those computers revealed fragments of Yahoo messages between Russell's Yahoo account and Rindfleisch's rellyk_us@yahoo.com account. In addition, emails obtained by search warrant from Russell's Google account "indicate[ ] that on numerous occasions, Rindfleisch forwards messages from her Milwaukee County e-mail account . . . to a private e-mail account at kmrindfleisch@gmail.com. In turn, . . . [Rindfleisch] sends those messages on to additional parties, including Tim Russell and persons associated with the Scott Walker campaign." The affidavit stated that "[m]any of these e-mails were sent during presumptive business days, Monday through Friday between 8 a.m. and 5 p.m." In addition, emails contained in Russell's timrussellwi@gmail.com account show he received a number of emails from Rindfleisch using rellyk_us@yahoo.com.

¶28 In a fact scenario similar to the case at bar, the United States Court of Appeals for the Ninth Circuit, in ***United States v. Adjani***, 452 F.3d 1140

(9th Cir. 2006), concluded that a search warrant to search the electronic files of Jana Reinhold passed constitutional muster. In that case, the government applied for a warrant to search Reinhold's electronic files based on her connection to Christopher Adjani. ***Id.*** at 1142. Adjani was suspected of threatening to sell confidential payment information from Paycom Billing Services. ***Id.*** at 1143. Based in part on e-mail communications discovered between Adjani and Reinhold, both were charged with conspiring to commit extortion and transmitting a threatening communication with intent to extort. ***Id.*** at 1142. Both Adjani and Reinhold moved to suppress specific emails between them, discovered via Reinhold's personal hard drive, arguing that the warrant lacked probable cause because the warrant did not label Reinhold as a suspect. ***Id.*** at 1146-47.

¶29 In a decision reversing the federal district court, the Ninth Circuit concluded that the warrant stated sufficient probable cause because the warrant was only required to establish probable cause to believe that evidence of the crimes at issue could be found on Reinhold's hard drive, regardless of whether Reinhold was a suspect. ***Id.*** at 1147.[14]

[14] The Dissent appears to be of the view that because the affidavits supporting the email searches did not establish probable cause to believe *Rindfleisch* had committed a crime, the warrants violated her Fourth Amendment rights. *See* Dissent, ¶45.

(Continued on following page)

¶30 Likewise, the warrant at issue in this case established, in no uncertain terms, that the State sought evidence of two particular crimes – misconduct in public office and political solicitation involving public officials and employees. The warrant requested the production of the following items, as material to this case, to establish evidence that the two particular crimes at issue were committed by Russell:

- Additional email accounts discovered by the investigation which appear to be controlled by Russell;

The error in the Dissent's analysis is evident upon review not only of the United States Court of Appeals decision discussed above, but more compellingly upon review of the United States Supreme Court's opinion in ***Zurcher v. Stanford Daily***, 436 U.S. 547 (1978), where the Supreme Court explained:

> The Warrant Clause speaks of search warrants issued on "probable cause" and "particularly describing the place to be searched, and the persons or things to be seized." In situations where the State does not seek to seize "persons" but only those "things" which there is probable cause to believe are located on the place to be searched, there is no apparent basis in the language of the Amendment for also imposing the requirements for a valid arrest – probable cause to believe that the third party is implicated in the crime.

Id. at 554. The Court also observed that "the State's interest in enforcing the criminal law and recovering evidence is the same whether the third party is culpable or not." ***Id.*** at 555. Here, the affidavits established probable cause to believe that *Russell* had committed a crime, and probable cause to believe that evidence of *Russell's* crime probably could be found on emails Rindfleisch had sent to or received from Russell. More is not required by the Fourth Amendment.

- Accounts controlled by Rindfleisch, the current Deputy Chief of Staff in the Milwaukee County Executive's Office, which accounts are believed to contain evidence in the form of emails sent to and received by Russell; and
- Accounts controlled by Russell's roommate, Brian Pierick, which were believed to have evidence of Russell's political activity while Russell was serving as a Milwaukee County employee.

¶31 Like in ***Adjani***, the warrants at issue in this case sought items based on the probable cause to believe that specific crimes were committed. The scope was limited to evidence of misconduct in public office or political solicitation involving public officials and employees, in violation of WIS. STAT. §§ 946.12, 11.36, and 11.61.

3. Particularized description of the place to be searched and the items to be seized.

¶32 The two ISPs, Google and Yahoo, were specifically identified by name and address. The places within their data storage system were particularly described as "For the time period of January 1, 2009, to the present, this warrant applies to information associated with the account identified [in the warrant] stored at premises owned, maintained, controlled, or operated by" the particular ISP. Rindfleisch has offered no evidence suggesting that the search exceeded the locations here described.

¶33 As to the items to be seized, the affidavit identified specific email accounts – four with Yahoo and two with Google – with which the warrants were concerned. Two were accounts in Russell's name: tdrussell63@yahoo.com, and trussell@yahoo.com. One account was in Pierick's name, bpierick@yahoo.com. Two of the accounts were in Rindfleisch's name: rellyk_us@yahoo.com and kmrindfleisch@gmail.com. One account, scottforgov@gmail.com, was an account that Budde believed was actually controlled by Pierick, who was also a blogger for the Walker campaign.

¶34 Additionally, as we have seen, information held by the ISPs which specifically identified the owner of the accounts and the personal contact information associated with the accounts, was also requested. This was necessary to ensure that the accounts were not actually owned or controlled by someone other than the suspected owner.

¶35 Rindfleisch has offered no evidence suggesting that information beyond those requests was produced.

E. The ISPs returned their Electronic Information with an Oath or Afirmation [sic] that the Records Produced Complied with the Warrant.

¶36 As noted, when Google responded to the warrant, it stated:

> To the extent any document provided herein contains information exceeding the scope of your request, protected from disclosure or otherwise not subject to production, if at all, we have redacted such information or removed such data fields.

When Yahoo produced its records, it swore in an affidavit that:

> Pursuant to the Federal Stored Communications Act, 18 USC §§ 2701 et. Seq., we have redacted information, including removing certain data fields, that exceeds the scope of this request, is protected from disclosure or is otherwise not subject to production.

¶37 The Dissent relies on ***United States v. Ganias***, 755 F.3d 125, 134-135 (2d Cir. 2014), for the well-established general proposition that "The government is barred from accessing data not within the scope of the search warrant." *See* Dissent, ¶44 In ***Ganias***, federal agents made forensic mirror images of Stavros Ganias's hard drives. ***Id.*** at 128-29. The record in ***Ganias*** included findings that the agents knew they could not have access to the information on the hard drive image not covered by the warrant, and that they carefully separated the covered information from that not covered. ***Id.*** at 137-38. However, instead of returning the information from the hard drive image not covered by the warrant, the government kept it. ***Id.*** at 138. Three years later, another government agency used the improperly retained hard drive image to bring charges against the

defendant. ***Id.*** at 130. Predictably, that did not sit well with the court, which noted extensive facts in the record amounting to obvious government misconduct. ***Id.*** at 137-40. The record before this court permits no such findings. The ISPs asserted that they had complied with the warrant, and even that they had redacted information from their productions. Rindfleisch has not produced a shred of evidence to dispute those representations, has rejected the opportunity before this court to identify specific documents that she claimed were beyond the scope of the warrant, and has relied instead on rhetorical salvos attacking the entire scope of the warrants.

F. More is not required here by the Fourth Amendment simply because the Evidence seized is Electronic Data.

¶38 Rindfleisch urges this court to adopt the protocol described in ***In the Matter of the United States Of America's Application For A Search Warrant To Seize And Search Electronic Devices From Edward Cunnius***, 770 F. Supp. 2d 1138 (W.D. Wash. 2011),[15] a memorandum order by a federal magistrate judge. In that case, Edward Cunnius was suspected of selling counterfeit Microsoft technology.

---

[15] As of the writing of this opinion, the only cases that have considered ***In the Matter of the United States Of America's Application For A Search Warrant To Seize And Search Electronic Devices From Edward Cunnius***, 770 F. Supp. 2d 1138 (W.D. Wash. 2011), have declined to follow it.

Id. at 1139. The government applied for a search warrant to search, among other things, all of Cunnius's electronically stored information. ***Id.*** at 1139-1140. The magistrate judge found the requested warrant overbroad because the warrant made no reference to the use of a filtering agent to sort through all of the electronic evidence. ***Id.*** at 1141.

¶39 Rindfleisch argues, based on ***Cunnius,*** that the Fourth Amendment, as applied to electronic communications, should be read to require an extra layer of protection not historically accorded paper documents, namely an electronic "filter" (the details of which she does not specify) to keep her "personal" or "private" material from being disclosed. She has identified no specific "personal" or "private" material that has been improperly produced. Alternatively, still based on ***Cunnius,*** she suggests that a third party should have been appointed by the warrant-issuing judge to review what Google and Yahoo produced. That third person would be the arbiter of what, within the data produced, would be available to the government. We are not persuaded.

¶40 The Fourth Amendment parameters of search and seizure law, largely developed in the context of obtaining tangible evidence, are not necessarily inapplicable to all searches for and seizures of electronic information. For example, a search warrant for a filing cabinet, located in a particular place, which contains a year's worth of correspondence between, or relating to, two particular individuals, would normally be searched where the filing cabinet

is located by the officers executing the warrant. Likewise, many documents in that filing cabinet would have nothing to do with either of those individuals. The only way the officer could distinguish between what relates to either of those individuals and what does not, is to look through all of the documents in the filing cabinet. Law enforcement officers have long had to separate the documents as to which seizure was authorized from the other documents. So far, as we have been able to discover, that necessity has not turned an otherwise valid warrant into a "general" warrant. We see no constitutional imperative that would change the result simply because the object of the search is electronic data from a specific electronic file, for a reasonably specific period of time, in the custody of a specific ISP.

¶41 Further, in this case, both ISPs stated in writing essentially the same thing: that they provided *only* what was required by the warrant, and they removed electronic data beyond the scope of the warrant. Rindfleisch had the opportunity before the circuit court to identify specifically what evidence she believed was improperly seized. She elected not to do so, and instead argued that the warrant on its face did not satisfy the Fourth Amendment.[16]

[16] Rindfleisch moved to seal the documents in the record. Third-party media entities moved to intervene to oppose the motion. We allowed the third-party entities to intervene and asked Rindfleisch to identify which documents she wished to seal as being beyond the scope of the warrants. Rindfleisch,

(Continued on following page)

CONCLUSION

¶42 Rindfleisch has failed to present any evidence at any time during these proceedings that tends to suggest that her Fourth Amendment rights were violated by the seizure authorized in these warrants. We have concluded that the State established, as the circuit court found, that the warrants in question were based on probable cause established by affidavit, were authorized by a judge, and particularly described the place to be searched and items to be seized. We therefore conclude, as did the circuit court, that the warrants at issue satisfy all of the requirements of the Fourth Amendment. We further find no evidence in this record suggesting in any way that the ISPs provided information beyond the scope of the warrant, much less that the information produced was in flagrant disregard of the scope of the warrant. Consequently, the circuit court's refusal to suppress everything obtained by the State from the ISPs was properly denied.

By the Court. – Judgment affirmed.

Recommended for publication in the official reports.

---

through counsel, declined to do so, asserting that such a search would be too time-consuming and expensive.

No. 2013AP362(D)

¶43 FINE, J. (*dissenting*). The essence of our country is "that a law repugnant to the constitution is void; and that *courts,* as well as other departments, are bound by that instrument." ***Marbury v. Madison,*** 1 Cranch 137, 180 (1803). (Emphasis in original.) Simply put, we are governed by our Constitution, not expediency.

A. *Search.*

¶44 We are bound by the Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.

The Supreme Court has explained:

> The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one "particularly describing the place to be searched and the persons or things to be seized." The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, 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. Thus, the scope of a lawful search is "defined by the object of the search and the places in which there is probable cause to believe that it may be found."

Maryland v. Garrison, 480 U.S. 79, 84 (1987) (quoted sources and footnote omitted). Yet, the Majority eschews the Fourth Amendment's command and permits the government to rummage through Kelly Rindfleisch's digital files for evidence of *her* crime even though the search warrants sought evidence in those files of *another's crime by another person* (Tim Russell) and lacked probable cause to believe that Rindfleisch's digital files had *any* evidence of *any* crime that Rindfleisch might have committed. *See* ***Arizona v. Gant***, 556 U.S. 332, 345 (2009) (The Framers were "concern[ed] about giving police officers unbridled discretion to rummage at will among a person's private effects.") (footnote omitted).

> The Fourth Amendment guards against this practice by providing that a warrant will issue only if: (1) the Government establishes probable cause to believe the search will uncover evidence of a *specific* crime; and (2) the warrant states with particularity the areas to be searched and *the items to be seized.* The latter requirement, in particular, "makes general searches . . . impossible" because it "prevents the seizure of one thing under a warrant describing another." This restricts

> the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item not described in the warrant.

United States. v. Ganias, 755 F.3d 125, 134-135 (2d Cir. 2014) (emphasis added, quoted sources and citations omitted; ellipses in ***Ganias***) (The government is barred from accessing data not within the scope of the search warrant.). Contrary to this enshrined Fourth-Amendment law, the search warrants for Rindfleisch's digital files did not:

- set out probable cause that Rindfleisch had done anything wrong (as the Fourth Amendment requires); and
- describe any place where any evidence that she had done anything wrong could be found (as the Fourth Amendment also requires).

The danger in this type of case is palpable:

> [B]ecause there is currently no way to ascertain the content of a file without opening it and because files containing evidence of a crime may be intermingled with millions of innocuous files, "[b]y necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there." Once the government has obtained authorization to search the hard drive, the government may claim that the contents of every file it chose to open

> were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant. There is, thus, "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches.

United States v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013) (quoted sources omitted; second set of brackets in ***Galpin***). Rindfleisch's lawyer told us at oral argument that of the approximately 16,000 documents received from the Rindfleisch email accounts pursuant to the search warrants "there were probably" fewer "than 500 pieces of paper that had Kelly Rindfleisch's political involvement in them." The State thus hardly "inadvertently" stumbled on the ream of pages that led to Rindfleisch's charges. *See* ***Coolidge v. New Hampshire***, 403 U.S. 443, 469-470 (1971) (The "plain view" doctrine does not apply to the government's discovery of implicating material that is not covered by a search warrant if the discovery was not "inadvertent.").

¶45 The Fourth Amendment prohibits the government to legitimately go into a person's voluminous files looking for evidence that *someone else* may have violated the law (here, Russell, the search warrants' object), and then root around those voluminous files to see if the subpoenas' subject (here Rindfleisch) may have also violated the law. Yet, the

State admits in its brief that it did precisely that: "As the warrants and supporting affidavit make clear, however, the John Doe investigation had targeted Tim Russell, not Rindfleisch, and the warrants sought Rindfleisch's communications for the purpose of filling gaps in Russell's e-mail communications." Also, the State was asked at oral argument:

> Court of Appeals Judge: "But there was no probable cause stated in the affidavits [in support of the search warrants] to believe under the Fourth Amendment that Ms. Rindfleisch was guilty of a crime."
>
> Assistant Attorney General: "Right. At that point. . . . As far as I know they [the prosecutors] did not have any belief that Ms. Rindfleisch or anybody else that was engaged in this kind of conduct [other than Russell, whose emails in Rindfleisch's accounts were sought by the search warrants]. That [Rindfleisch's alleged culpability] became apparent after they [the prosecutors] got the return on the warrant for the documents that were within the scope of the warrant[s] that were approved [namely, for the search of Russell's emails in Rindfleisch's digital accounts]."

(Formatting modified.) The search of Rindfleisch's voluminous digital files was illegal because the search warrants were silent as to whether there was probable cause to believe that she was culpable.

B. *Suppression.*

> Even where a search or seizure violates the Fourth Amendment, the Government is not automatically precluded from using the unlawfully obtained evidence in a criminal prosecution. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Suppression is required "only when [agents] (1) . . . effect a widespread seizure of items that were not within the scope of the warrant, and (2) do not act in good faith."
>
> The Government effects a "widespread seizure of items" beyond the scope of the warrant when the Government's search "resemble[s] a general search." Government agents act in good faith when they perform "searches conducted in objectively reasonable reliance on binding appellate precedent." When Government agents act on "good-faith reliance [o]n the law at the time of the search," the exclusionary rule will not apply. "The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance."

Ganias, 755 F.3d at 136-137 (quoted sources and citations omitted, brackets and ellipses in ***Ganias***). Here, the exclusionary rule thus applies because: (1) the State both widely and knowingly exceeded the scope of the Rindfleisch search warrants that sought

only the Russell emails, and (2) the State did not objectively act in good faith based on Fourth-Amendment law that was clear at the time of the search.

C. *Conclusion.*

¶46 The Majority legitimizes a general warrant and nullifies our Constitution. I respectfully dissent and would grant Rindfleisch's motion to suppress the data provided pursuant to the search warrants that concerned Rindfleisch and not Russell. *See* ***State v. Petrone***, 161 Wis. 2d 530, 548, 468 N.W.2d 676, 682-683 (1991) ("The general rule is that items seized within the scope of the warrant [here, relating to Russell] need not be suppressed simply because other items outside the scope of the warrant [here, relating to Rindfleisch] also were seized, unless the entire search was conducted in 'flagrant disregard for the limitations' of the warrant.") (footnotes omitted, brackets supplied).

STATE OF WISCONSIN	CIRCUIT COURT BRANCH 42	MILWAUKEE COUNTY	*For Official Use Only*
of Wisconsin vs. M. Rindfleisch	**Judgment of Conviction** Sentence Withheld, Probation Ordered		**FILED** **11-27-2012** **John Barrett** **Clerk of the Circuit Court**
of Birth: [Omitted In Printing]	Case No. 2012CF000438		

The defendant was found guilty of the following crime(s):

Description	Violation	Plea	Severity	Date(s) Committed	Trial To	Date(s) Convicted
Misconduct/Office	946.12(3)	Guilty	Felony I	04-14-2010		10-11-2012

T IS ADJUDGED that the defendant is guilty as convicted and sentenced as follows:

Sent. Date	Sentence	Length	Agency	Comments
11-19-2012	Probation, sent withheld	3 YR	Department of Corrections	Court will allow probation and condition time to be transferred to Columbia County.

itions of Sentence or Probation
bligations: (Total amounts only)

Court Costs	Attorney Fees	☐ Joint and Several Restitution	Other	Mandatory Victim/Wit. Surcharge	5% Rest. Surcharge	DNA Anal. Surcharge
20.00			13.00	92.00		250.00

itions

Condition	Length	Agency/ Program	Begin Date	Begin Time	Comments
House of Correction	6 MO				Release for work and family healthcare. STAYED pending appeal.

Condition	Agency/ Program	Comments
Costs		Provide DNA sample if one has not previously been provided, pay surcharge. Pay all court costs, fees and surcharges. Failure to pay shall result in entry of a civil judgment.
Other		Standard rules of probation.
Firearms/ Weapons Restriction		Defendant advised as a convicted felon she may never possess a firearm or body armor; her voting privileges are suspended and she may not vote in any election until her civil rights are restored.

uant to §973.01(3g) and (3m) Wisconsin Statutes, the court determines the following:
Defendant is ☐ is not ☐ eligible for the Challenge Incarceration Program.
Defendant is ☐ is not ☐ eligible for the Substance Abuse Program.

ollowing charges were Dismissed but Read In

Description	Violation	Plea	Severity	Date(s) Committed	Date(s)Convicted
Misconduct/Office	946.12(3)		Felony I	04-16-2010	10-11-2012
Misconduct/Office	946.12(3)		Felony I	05-03-2010	10-11-2012
Misconduct/Office	946.12(3)		Felony I	05-04-2010	10-11-2012

STATE OF WISCONSIN	CIRCUIT COURT BRANCH 42	MILWAUKEE COUNTY	*For Official Use Only*
State of Wisconsin vs. Kelly M. Rindfleisch	**Judgment of Conviction** Sentence Withheld, Probation Ordered		**FILED** **11-27-2012** **John Barrett** **Clerk of the Circuit Court**
Date of Birth: [Omitted In Printing]	Case No. 2012CF000438		

Distribution:

David A. Hansher-42, Judge
Bruce J Landgraf, District Attorney
Franklyn M Gimbel, Defense Attorney

[SEAL]

BY THE COURT:

Electronically signed by John Barrett
Circuit Court Judge/Clerk/Deputy Clerk

November 27, 2012
Date

STATE OF WISCONSIN | CIRCUIT COURT | MILWAUKEE COUNTY

STATE OF WISCONSIN,

Plaintiff,

vs. Case No. 12-CF-000438

KELLY M. RINDFLEISCH,

Defendant.

ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE OBTAINED VIA SEARCH WARRANTS

The Court having considered defendant Kelly M. Rindfleisch's motion for an order suppressing evidence obtained by the state via search warrants issued on October 20, 2010, including all pleadings and papers of record and the arguments of counsel, for the reasons set forth from the Bench on August 21, 2012, the motion is hereby DENIED.

Dated this 14th day of September, 2012.

BY THE COURT:

/s/ David A. Hansher
DAVID A. HANSHER
Circuit Court Judge

Drafted by:
Kathryn A. Keppel
Gimbel, Reilly, Guerin & Brown LLP
330 East Kilbourn Avenue
Milwaukee, Wisconsin 53202
Telephone: 414/271-1440
crim/rindfleisch/p/dimisssuppressorder2012-09-06

STATE OF WISCONSIN | CIRCUIT COURT BRANCH 42 | MILWAUKEE COUNTY

STATE OF WISCONSIN,

Plaintiff,

-vs- Case No. 12CF000438

KELLY M. RINDFLEISCH,

Defendant.

DECISION (EXCERPT)

August 21, 2012 Hon. David A. Hansher
Presiding

CHARGE

Counts 1-4: Misconduct in office.

APPEARANCES

Bruce Landgraf, Attorney at Law, appeared on behalf of the State of Wisconsin.

Franklyn Gimbel, Attorney at Law, appeared on behalf of the defendant, not present.

Kristin Menzia, RMR, CRR, Official Court Reporter

[2] **PROCEEDINGS**

(The following is an excerpt from Case No. 12CF000438:)

THE COURT: Okay. So I'm just doing to deal with the motion to suppress. Miss Rindfleisch has moved this court for an order suppressing all evidence obtained by the state via search warrants issued to Yahoo and Google. She seeks suppression on the grounds that the sweeping nature of the search warrant eviscerates her privacy rights under the Fourth and Fourteenth amendments and correlative provisions under the Wisconsin Constitution.

The warrants required an unknown employee of the commercial internet service provider, ISPs, to produce all of their records, and then left it to law enforcement officers to sift through Rindfleisch's personal private communications to determine which of those communications – which of those communications actually related to this case.

Although 968.375 provides the state the opportunity to obtain such electronic communication, enactment of the statute should not be construed to be an invitation for law [3] enforcement officers to ignore their requirements to particularize items such to the search. And that's the position of the defense.

The state responded by arguing that the motion must be denied for the following reasons. One, the warrants were not unconstitutionally overbroad. Two, even if the warrants were overbroad, suppression should only extend to those items outside the lawful scope of the search warrants. And three, the state has the e-mail accounts through an independent seizure of Miss Rindfleisch's laptop in November of 2010.

They claimed the e-mails are not solely the fruits of the warrant. And I'll deal with those issues and then deal with the reply brief issues and the rejoinder of the state.

The court – I find that there's no requirement that individuals acting pursuant to a search warrant prescreen bulk digital evidence. The only case originally cited by the defense – And other cases were cited in the reply. And I'll deal with that in a second. The only case originally cited by the defense for this proposition was United States versus Carey, C-A-R-E-Y, 172 F.3d 1268 from the 10th Circuit, [4] 1999.

The defendant cites a footnote within the opinion quoting a Harvard Law Journal that, quote, where a search warrant seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records, end of quote.

The reasoning, I find it in the original brief, is not persuasive because Rindfleisch does not contend that the law enforcement officers searched beyond the scope of her personal e-mail accounts for records related to the crimes she's been charged with.

Case law cited to by the state in their original brief supports the proposition that there's no pre-screening requirements for e-mail accounts under United States versus Bowen, B-O-W-E-N, 689 F.Supp.2d 675, which is from the Southern District of New York,

2010, and United States versus Taylor, 764 F.Supp.2d 230 from 2011.

The Fourth Amendment, according to those cases, does not require the government to [5] delegate a pre-screening function to the ISP, and I think the ISP is in brackets, or to ascertain which e-mails are relevant before copies are obtained for subsequent searchings. All supporting the state's – Also supporting the state's position is the Federal Rules of Criminal Procedure which supports its arguments that there's no pre-screening requirements.

And that's Federal Criminal Procedure Rule 41(e)(2)(B). That's a capital B by the way. Which provides a warrant may be authorized to seize – authorize the seizure of electronic media or the seizure of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the information consistent with the warrant.

Now, the defendant's reply brief from Friday or Monday cites U.S. versus, if I'm pronouncing it right, Cioffi, C-I-O-F-F-I, 668 F.2d 385, Eastern District of New York, 2009. And I find it's not on point and is a Federal District Court case and not a Federal Circuit Court decision, which I think might have more bearing on this case and more persuasive arguments.

[6] Furthermore, the search warrant in Cioffi was found to be overbroad. It was to search for evidence of a crime while here the search warrant was more limited for specific crimes of illegal campaign

activity which could lead to misconduct in public office charges, which eventually happened here.

Although I find Cioffi not on point, it did contain interesting and insightful thoughts about the Fourth Amendment computer searches. They observed that documents searches pose unique Fourth Amendment concerns in the context of the computer searches. Later they pointed out that the majority of courts – And I think they're talking about federal courts. I wasn't sure, but I think it's limited to federal courts – have considered the question and have not required the government to specify its search protocol in advance.

As it is now, the computer forensics process is too contingent and unpredictable for judges to establish effective anti rules. Anti, A-N-T-I. Anti basically are rules to be followed prior to the search of the computer. And I took these cases off the computer myself. And they [7] don't have pages on it since no federal cases were attached to the motion, I think inadvertently.

The Bowens case cited earlier by me in U.S. versus McDarrah, M-C capital D-A-R-R-A-H, 351 Fed App 558, from the 2nd Circuit, 2009, and State versus Taylor, which I cited previously, all support the state's contention that this warrant was not overly broad. And I find both of them on point.

The Ninth Circuit, the Ninth Federal Circuit in the Belcor cases, and those are the cases involving use of performance enhancing drugs in baseball, and

this I believe is the Federal Court out of San Francisco, have taken a narrow view of computer searches and might – might under the case of U.S. versus Comprehensive Testing, 621 F.3d, 1162, accept the defendant's arguments in this case. But I could not on such short notice find any other federal circuits, especially our own Seventh Circuit, that have or would have followed the Comprehensive Testing case rationale.

And see U.S. versus Mann, M-A-N-N, 592 F.3d 779, which takes a more broader view [8] from the Seventh Circuit. That's from 2010. It was decided before the Comprehensive Testing case of the Ninth Circuit, but I don't think it would change the decision of the Seventh Circuit. So at least there's a split between those circuits. But again, out of all the Circuit Courts, the Federal Circuit Courts and the United States, I only could find the Ninth Circuit which would follow the defendant's – would accept the defendant's arguments and I rejected them.

I find that the warrants here, when read as a whole, were appropriately specific and are not overbroad. I find that the warrants authorized the search of specific e-mail accounts for a specific time period for specific crimes which evidenced campaign activity by government employees. Even if the warrants were overbroad, I find the items are within the scope of the warrants – or the items within the scope of the warrants should not be suppressed because the search is not conducted in, quote, flagrant disregard for the limitations, end of quote, of the warrant.

Generally items seized within the scope of a warrant need not be suppressed simply [9] because other items outside the scope of the warrant were also seized, unless the entire search was conducted in a flagrant disregard for the limitations of the warrant. Again, that's from State versus Marten, 165 Wis. 2nd 70, Court of Appeals from 1991.

I therefore find, except for the Ninth Circuit, there is no case law which would require law enforcement officers to conduct an onsite inspection of the contents of a computer and copy relevant files and documents. I find such a requirement would be impractical and could take weeks, if not months, for a computer with a large volume of documents stored within it.

Lastly, the seized e-mails I find were later independently obtained through the seizure of Rindfleisch's laptop computer on November 1st, 2010. The laptop was seized pursuant to a search warrant issued by the John Doe judge for the Offices of the County Executive on November 1st, 2010.

For the foregoing reasons, the motion to suppress evidence obtained via the search warrants is denied and the motion to declare a 968.375 as unconstitutional is also denied. I [10] find there's no basis in fact or law to find it unconstitutional based upon the same rationale for suppressing the search warrant. Anything else from the state or the defense as to those motions?

MR. LANDGRAF: Not from the state, Judge.

MR. GIBEL [sic]: No, Your Honor.

– – – – – – –

(Proceedings excerpt concluded.)

SEARCH WARRANT **MILWAUKEE, WISCONSIN**

CIRCUIT COURT
FIRST JUDICIAL DISTRICT

STATE OF WISCONSIN) In the Circuit Court
) ss. of the First Judicial
MILWAUKEE COUNTY) District of Wisconsin

(Filed Oct. 20, 2010)

The State of Wisconsin, to any Sheriff, or any Law Enforcement officer of the State of Wisconsin:

WHEREAS, 1. ☐ oral testimony was presented to the Circuit Court Branch of the First Judicial District and recorded by a stenographic reporter on , and

WHEREAS, 2. ☒ David E. Budde has complained (by attached affidavit) to this court upon oath,

Showing probable cause that on today's date within the jurisdiction of the State of Wisconsin and this John Doe proceeding as set forth in Wisconsin Statutes §968.375(2), there is now located certain electronic communication service records described as follows:

RECORDS TO BE PRODUCED: For the time period of January 1, 2009 to the present, this warrant applies to information associated with the account identified as rellyk_us@yahoo.com stored at premises owned, maintained, controlled, or operated by Yahoo, Inc., a company headquartered at 701 First Avenue, Sunnyvale, California 94089. This warrant requires,

ON OR BEFORE NOVEMBER 22, 2010 the production of:

a. The contents of all communications stored in the Yahoo accounts for the subscriber(s) identified above, including all emails stored in the account, whether sent from or received in the account as well as e-mails held in a "Deleted" status;

b. All records or other information regarding the identification of the accounts, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account statuses, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records pertaining to communications between Yahoo, Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

THIS WARRANT MAY BE COMPLIED WITH BY DELIVERING RECORDS TO CHIEF INVESTIGATOR DAVID BUDDE, MILWAUKEE COUNTY DISTRICT ATTORNEY'S OFFICE, ROOM 405, 821 WEST STATE STREET, MILWAUKEE, WISCONSIN. QUESTIONS CONCERING [sic] THIS WARRANT MAY BE DIRECTED TO ASSISTANT

DISTRICT ATTORNEY HANNA R. KOLBERG, (414) 278-4301 or hanna.kolberg@da.wi.gov:

DESCRIBE OBJECTS OF LAW ENFORCEMENT SEARCH:

This warrant authorizes law enforcement officers to search the information described above for the following evidence of crime:

a. For the time period of January 1, 2009 to the present, all records relating to Misconduct in Public Office and Political Solicitation involving Public Officials and Employees, violations of §§946.12, 11.36 and 11.61 of the Wisconsin Statutes, including information relating to the financial or other benefit provided to any private and/or political cause or organization either effected using Milwaukee County facilities or effected during periods of normal county work hours or both.

The terms "records" and "information" include all items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage.

Which objects constitute evidence of the commission of a crime, to wit;

DESCRIBE CRIME OR CRIMES:

(1) Misconduct in Public Office; and

(2) Political Solicitation involving Public Officials and Employees committed in violation of sections 946.12, 11.36 and 11.61 of the Wisconsin Statutes.

Now, THEREFORE, in the name of the State of Wisconsin, you are commanded forthwith to search the said premises and/or the said person(s) for said things, and take possession thereof, if found.

I further order that this search warrant shall be returned as provided in Wisconsin Statutes §968.375(11) directly to Circuit Court, Room 609, Courthouse, 901 North 9th Street, Milwaukee, where it shall be maintained under seal in Case No. 10JD000007.

THIS JOHN DOE SEARCH WARRANT IS ISSUED SUBJECT TO A SECRECY ORDER. BY ORDER OF THE COURT, PURSUANT TO A SECRECY ORDER THAT APPLIES TO THIS PROCEEDING, YOU ARE HEREBY COMMANDED AND ORDERED NOT TO DISCLOSE TO ANYONE, OTHER THAN YOUR OWN ATTORNEY, THE CONTENTS OF THIS SEARCH WARRANT AND/OR THE FACT THAT YOU HAVE RECEIVED THIS SEARCH WARRANT. VIOLATION OF THIS SECRECY ORDER IS PUNISHABLE AS CONTEMPT OF COURT.

Witness, the Hon. Neal Nettesheim, Reserve Judge for the First Judicial District of Wisconsin, at 3 ~~a.m.~~/p.m. on October 19, 2012.

/s/ Neal Nettesheim
Honorable Neal Nettesheim
Reserve Judge of the
Circuit Court

[SEAL]

SEARCH WARRANT **MILWAUKEE, WISCONSIN**

CIRCUIT COURT
FIRST JUDICIAL DISTRICT

STATE OF WISCONSIN) In the Circuit Court
) ss. of the First Judicial
MILWAUKEE COUNTY) District of Wisconsin

(Filed Oct. 20, 2010)

The State of Wisconsin, to any Sheriff, or any Law Enforcement officer of the State of Wisconsin:

WHEREAS, 1. ☐ oral testimony was presented to the Circuit Court Branch of the First Judicial District and recorded by a stenographic reporter on , and

WHEREAS, 2. ☒ David E. Budde has complained (by attached affidavit) to this court upon oath,

Showing probable cause that on today's date within the jurisdiction of the State of Wisconsin and this John Doe proceeding as set forth in Wisconsin Statutes §968.375(2), there is now located certain electronic communication service records described as follows:

RECORDS TO BE PRODUCED: For the time period of January 1, 2009 to the present, this warrant applies to information associated with the account identified as kmrindfleisch@gmail.com stored at premises owned, maintained, controlled, or operated by Gmail (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA, 94043.

This warrant requires, **ON OR BEFORE NOVEMBER 22, 2010** the production of:

a. The contents of all communications stored in the Gmail accounts for the subscriber(s) identified above, including all emails stored in the account, whether sent from or received in the account as well as e-mails held in a "Deleted" status;

b. All address books, contact lists, friends lists, buddy lists, or any other similar compilations of personal contact information associated with the accounts;

c. All records or other information regarding the identification of the accounts, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account statuses, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records pertaining to communications between Gmail (Google), and any person regarding the accounts, including contacts with support services and records of actions taken.

THIS WARRANT MAY BE COMPLIED WITH BY DELIVERING RECORDS TO CHIEF INVESTIGATOR DAVID BUDDE, MILWAUKEE COUNTY

DISTRICT ATTORNEY'S OFFICE, ROOM 405, 821 WEST STATE STREET, MILWAUKEE, WISCONSIN. QUESTIONS CONCERING [sic] THIS WARRANT MAY BE DIRECTED TO ASSISTANT DISTRICT ATTORNEY HANNA R. KOLBERG, (414) 278-4301 or hanna.kolberg@da.wi.gov:

DESCRIBE OBJECTS OF LAW ENFORCEMENT SEARCH:

This warrant authorizes law enforcement officers to search the information described above for the following evidence of crime:

a. For the time period of January 1, 2009 to the present, all records relating to Misconduct in Public Office and Political Solicitation involving Public Officials and Employees, violations of §§946.12, 11.36 and 11.61 of the Wisconsin Statutes, including information relating to the financial or other benefit provided to any private and/or political cause or organization either effected using Milwaukee County facilities or effected during periods of normal county work hours or both.

The terms "records" and "information" include all items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage.

Which objects constitute evidence of the commission of a crime, to wit;

DESCRIBE CRIME OR CRIMES:

(1) Misconduct in Public Office; and

(2) Political Solicitation involving Public Officials and Employees committed in violation of sections 946.12, 11.36 and 11.61 of the Wisconsin Statutes.

Now, THEREFORE, in the name of the State of Wisconsin, you are commanded forthwith to search the said premises and/or the said person(s) for said things, and take possession thereof, if found.

I further order that this search warrant shall be returned as provided in Wisconsin Statutes §968.375(11) directly to Circuit Court, Room 609, Courthouse, 901 North 9th Street, Milwaukee, where it shall be maintained under seal in Case No. 10JD000007.

THIS JOHN DOE SEARCH WARRANT IS ISSUED SUBJECT TO A SECRECY ORDER. BY ORDER OF THE COURT, PURSUANT TO A SECRECY ORDER THAT APPLIES TO THIS PROCEEDING, YOU ARE HEREBY COMMANDED AND ORDERED NOT TO DISCLOSE TO ANYONE, OTHER THAN YOUR OWN ATTORNEY, THE CONTENTS OF THIS SEARCH WARRANT AND/OR THE FACT THAT YOU HAVE RECEIVED THIS SEARCH WARRANT. VIOLATION OF THIS SECRECY ORDER IS PUNISHABLE AS CONTEMPT OF COURT.

Witness, the Hon. Neal Nettesheim, Reserve Judge for the First Judicial District of Wisconsin, at 3 ~~a.m.~~/p.m. on October 19, 2012.

/s/ Neal Nettesheim
Honorable Neal Nettesheim
Reserve Judge of the
Circuit Court

[SEAL]

OFFICE OF THE CLERK

Supreme Court of Wisconsin

110 EAST MAIN STREET, SUITE 215
P.O. BOX 1688
MADISON, WI 53701-1688

TELEPHONE (608) 266-1880
FACSIMILE (608) 267-0640
Web Site: www.wicourts.gov

March 16, 2015

To:

Hon. David A. Hansher
Milwaukee County
Circuit Court Judge
901 N. 9th St.
Milwaukee, WI 53233

John Barrett
Milwaukee County
Clerk of Circuit Court
821 W. State St., Rm. 114
Milwaukee, WI 53233

Franklyn M. Gimbel
Kathryn A. Keppel
Gimbel, Reilly, Guerin
& Brown
330 E. Kilbourn Ave.,
Ste. 1170
Milwaukee, WI 53202

Karen A. Loebel
Asst. District Attorney
821 W. State St.
Milwaukee, WI 53233

Christopher G. Wren
Assistant Attorney General
P.O. Box 7857
Madison, WI 53707-7857

Colleen Ball
State Public
Defender's Office
Appellate Division
735 N. Water St., #912
Milwaukee, WI 53202

Robert J. Dreps
Godfrey & Kahn, S.C.
P.O. Box 2719
Madison, WI 53701-2719

You are hereby notified that the Court has entered the following order:

No. 2013AP362-CR *State v. Rindfleisch*
L.C.#2012CF438

A petition for review pursuant to Wis. Stat. § 808.10 having been filed on behalf of defendant-appellant-petitioner, Kelly M. Rindfleisch, and considered by this court;

IT IS ORDERED that the petition for review is denied, without costs.

Prosser, J., did not participate.

Diane M. Fremgen
Clerk of Supreme Court

Constitutional Provisions And Statutes

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.

Fourth Amendment, United States Constitution

All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Fourteenth Amendment, Section 1, United States Constitution

Misconduct in public office. Any public officer or public employee who does any of the following is guilty of a Class I felony:

* * *

(3) Whether by act of commission or omission, in the officer's or employee's capacity as such officer or employee exercises a discretionary power in a manner inconsistent with the duties of the

officer's or employee's office or employment or the rights of others and with intent to obtain a dishonest advantage for the officer or employee or another. . . .

Wis. Stat. §946.12(3).
