STATE OF WISCONSIN

I N S U P R E M E C O U R T

Case No. 2013AP362-CR

STATE OF WISCONSIN,

Plaintiff-Respondent,

v.

KELLY M. RINDFLEISCH,

Defendant-Appellant-Petitioner.

STATE PUBLIC DEFENDER'S AMICUS CURIAE BRIEF IN SUPPORT OF KELLY M. RINDFLEISCH'S PETITION FOR REVIEW

KELLI S. THOMPSON
State Public Defender
State Bar No. 1025437

COLLEEN D. BALL
Assistant State Public Defender
State Bar No. 1000729

Office of the State Public Defender
735 North Water Street, Suite 912
Milwaukee, WI 53202-4116
(414) 227-3110
Email: ballc@opd.wi.gov

Attorneys for the State Public Defender

TABLE OF CONTENTS

CASES CITED

CONSTITUTIONAL PROVISIONS AND STATUTES CITED

OTHER AUTHORITIES CITED

INTRODUCTION

This case marks another collision on "the increasingly busy intersection between Fourth Amendment privacy considerations and the constant advancement of electronic technology." ***State v. Subdiaz-Osorio***, 2014 WI 87, ¶2, 357 Wis. 2d 41, 849 N.W.2d 748. The issue is how the breadth and particularity provisions of the Fourth Amendment and Article I § 11 of the Wisconsin Constitution apply to a warrant to search the email of a person who is not suspected of a crime, when that email is stored on the server of an Internet Service Provider such as Google or Yahoo.

"Among online adults, 92% use email, with 61% using it on an average day."[1] The court of appeals split decision in this case was just published. It thus affects most Wisconsinites, including law-abiding citizens who may unwittingly receive, forward, or even delete email messages containing evidence that the someone—perhaps someone they don't even know—committed a crime. The State may now seize the innocent citizen's entire email account, search it in secret,[2] and, judging from what occurred here, retain all of the seized email for future perusal. The implications of the court of appeals decision are alarming. This Court is the appropriate one to resolve an issue of such magnitude.

---

[1] Kristen Purcell, ***Search and Email Still Top the List of Most Popular Online Activities***, Pew Research Center Internet Project, available at http://www.pewinternet.org/2011/08/09/search-and-email-still-top-the-list-of-most-popular-online-activities/ (last visited 1/8/15).

[2]The State obtained these warrants pursuant to Wis. Stat. §968.375, which authorizes judges to issue them secretly and to prohibit the ISP from disclosing the existence of the warrant to the account owner. Wis. Stat. §968.375(10).

INTEREST OF AMICUS CURIAE

The State Public Defender is an independent, executive branch agency and law office that provides legal representation to the indigent in criminal cases throughout Wisconsin. The SPD's mission is to provide high-quality, compassionate and cost-effective legal representation, to protect the rights of the accused, and to advocate for a fair and rational criminal justice system.

The SPD litigates more criminal cases than any other law firm in Wisconsin. In 2013, it appointed counsel in over 138,000 cases involving indigent defendants. Most of those were assigned to the SPD's own trial and appellate lawyers. Given the volume and nature of cases it handles, the SPD has become Wisconsin's expert on criminal defense, including search-and-seizure law. The SPD is thus well-suited to explain the ramifications of the court of appeals decision for Wisconsin.

ARGUMENT

I. The Court of Appeals Decision Contains Significant Errors.

A. The majority decision misunderstands the warrants.

During a John Doe investigation, the State sought evidence that Tim Russell, Scott Walker's Chief of Staff when he was Milwaukee County Executive, had committed various alleged crimes. Toward that end, the State applied for and received search warrants regarding the personal Google and Yahoo email accounts of Kelly Rindfleisch, another

Milwaukee County employee, with the hope of finding evidence of Russell's crimes.

It is important to understand just what the warrants required of Google and Yahoo (the Internet Service Providers or "ISPs") on the one hand, and of law enforcement on the other, because the court of appeals majority opinion seems confused on that point. The majority wrote:

> 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.

State v. Rindfleisch, Appeal No. 2013AP362-CR, Slip op. ¶9 (Wis. Ct. App. Nov. 12, 2014)(emphasis supplied). This suggests that the ISPs were to examine Rindfleisch's email accounts, locate those that pertained to Russell's alleged crimes, and produce only those emails to the investigating officers. That is not what the warrants say.

In fact, as Rindfleisch's petition for review notes, the warrants ordered Google and Yahoo to produce literally ***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. (Rindfleisch Petition App.142-147). That amounted to 16,000 documents of personal communications. Slip op. ¶44. The warrant did ***not*** direct Google and Yahoo to search those 16,000 documents for evidence of Tim Russell's alleged crimes. It assigned that task to law enforcement:

> 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* . . .

(Rindfleisch App.142, 145)(emphasis supplied).

By directing Google and Yahoo to produce all of Rindfleisch's personal email on their servers, the warrants allowed law enforcement to "seize the haystack to look for the needle"—here, evidence of Russell's misconduct. ***United States v. Hill***, 459 F.3d 966, 975 (9th Cir. 2006).

B. The majority decision includes analytical errors that will confuse circuit courts addressing this issue.

The question in this case is whether the language of the warrants used to seize and search Rindfleisch's entire Google and Yahoo email accounts was too broad and/or insufficiently particular to satisfy the Fourth Amendment and Article I, §11 of the Wisconsin Constitution. The majority repeatedly lost sight of this issue, included stray reasoning, and now its decision stands as published precedent.

For example, the majority zeroed in on searches that police conducted in flagrant disregard for the limitations found in the underlying warrants. Slip op. ¶22. But the issue here is not whether the police violated the warrant; it's

whether the terms of the warrant violated the state and federal constitutions.

The majority stressed that the ISPs swore under oath that they complied with the warrants and produced only what the warrants required of them. Slip op. ¶¶36-41. That's not the issue either. The issue is whether the warrants directed the ISPs to produce—and thus allowed the investigating officers to seize—more than the state and federal constitutions permitted.

The majority also repeatedly chastised Rindfleisch for failing to prove which of the 16,000 emails produced and searched exceeded the scope of the warrants:

> Rindfleisch has not produced a shred of evidence to dispute those representations [that the ISPs had complied with the warrants], 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 warrant.

Slip op. ¶37. *See also* ¶¶32, 35, 39 & 41.

Again the majority missed the point. Rindfleisch challenged the terms of the warrants. This posed a question of law, not a question of fact that she had to prove. *See* ***State v. Meyer***, 216 Wis. 2d 729, ¶18, 576 N.W.2d 260 (1998)("Whether the language of the warrant satisfies the requisite constitutional requirements is a question of law. We review such issues of constitutional guarantees *de novo*.")

C. The majority decision overlooks the vigorous, national debate over how the Fourth Amendment should apply to the search and seizure of stored email to ensure both effective law enforcement and protection of the individual's privacy interests.

Consider what happens 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). Should 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).

Shrugging off these concerns, the majority held that the "seize then search" of an entire email account is just like a "search then seize" of incriminating-only letters in a filing cabinet:

> [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,[3] 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.[4] 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.*[5] *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.*

Slip op. ¶40 (emphasis supplied).

Many courts and legal scholars vehemently dispute this conclusion. Orin Kerr, an expert in this field, has explained at length how physical space differs from Internet space and argues that these differences require courts to find new ways to maintain the function of the Fourth Amendment in an online environment. Orin S. Kerr, ***Applying the Fourth***

---

[3] The warrants here were not confined to emails between two specific people. They ordered Google and Yahoo to turn over *all* email on Rindfleisch's accounts for specified periods of time.

[4] True, but someone would have initially decided which letters to place in the file cabinet and which letters to discard or store elsewhere. Not so with an email account sitting on Google's or Yahoo's servers, which preserve even deleted messages.

[5] But when this involves a vast quantity of intermingled documents, some courts require law enforcement to separate out what the investigating agents are permitted to view and retain. *See .e.g*. ***United States v. Ganias***, 755 F.3d 125, 135 (2d Cir. 2014); ***United States v. Tamura***, 694 F.2d 591, 595-96 (9th Cir. 1982); ***United States v. Carey***, 172 F.3d 1268, 1275 (10th Cir. 1999).

Amendment to the Internet: A General Approach, 62 Stan. L. Rev. 1005, 1007 (April 2010). *See also* Friess, ***When Rummaging Goes Digital***, at 1010-1011 (explaining the differences between the search of a physical space and the search of a digital space).

Scholars have noted that the admissibility of evidence discovered in "plain view" during a digital search raises concerns about the very "general searches" that the Fourth Amendment's particularity requirement was supposed to avert. Because there are many low-level offenses for which probable cause is easy to establish, law enforcement can easily target people. *See* Acharya, ***Semantic Searches***, at 401-402; 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).

Courts have likewise observed that if the government must open every electronic file on a computer to know its contents, then everything the government chooses to open will come into plain view. The Ninth Circuit thus 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. ***United States. v. Comprehensive Drug Testing, Inc.*** 621 F.3d 1162, 1167 (9th Cir. 2010). The concurrence went so far as to suggest that investigators seeking warrants to search electronic files forswear reliance on the "plain view" doctrine. ***Id*** at 1178 (Kozinski, J. concurring).

Another scholar observed that the lack of guidance from the United States Supreme Court has caused the circuits

to set out contradictory visions of the appropriate scope of a digital search. 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). The Ninth Circuit endorses a data segregation strategy. The Fourth and Tenth Circuits use the "file cabinet" analogy. The Seventh Circuit examines the search protocol used in light of the search authorized by the warrant. ***Id*** at 304. Some district courts are asking magistrate judges to require warrants to outline the protocols that will 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 short, the majority was mistaken. Rindfleisch's arguments are not just "rhetorical salvos." There is a national debate over whether a warrant directing an ISP to give investigating officers an entire email account so they may search every last byte for evidence of a crime is, in effect, a "general warrant" in violation of the Fourth Amendment. Thus, this case poses the logical follow up question to ***Riley v. California***, __U.S.__, 134 S.Ct. 2473 (2014). Now that a warrant is required to search digital data on a cell phone, for example, how broad or particular should that warrant be?

II. This Case Meets the Criteria for Wisconsin Supreme Court Review.

This is the first Wisconsin case to address how the Fourth Amendment's breadth and particularity provisions should apply to warrants to search stored email. Only two Wisconsin decisions mention Wis. Stat. § 968.375, the statute that authorizes subpoenas and warrants for electronic communications, and neither addresses the issue presented

here. *See* ***State v. Subdiaz-Osorio***, 2014 WI 87, 357 Wis. 2d 41, 849 N.W.2d 748; ***State v. Tate***, 2014 WI 89, 357 Wis. 2d 172, 849 N.W.2d 798. Indeed, a simple, "plain language" interpretation of §968.375(3) may solve the constitutional problem. That provision authorizes a warrant directing an ISP to disclose "the content" of "an electronic communication" (singular) not communications (plural), suggesting that the wholesale seizure of an email account exceeds the statute. There is no Wisconsin case law on point.

Resolution of these issues requires weighing the privacy rights of Wisconsin citizens against law enforcement investigation strategies. This Court, not the court of appeals, should decide how to strike the right balance. *See* Wis. Stat. §809.62(1r)(a), (b), and (c).

CONCLUSION

For the reasons stated above, the State Public Defender respectfully requests that the Wisconsin Supreme Court grant Kelly Rindfleisch's petition for review.

Dated this 13th day of January, 2015.

Respectfully submitted,

COLLEEN D. BALL
Assistant State Public Defender
State Bar No. 100729

Office of the State Public Defender
735 North Water Street, Suite 912
Milwaukee, WI 53202-4116
(414) 227-3110
E-mail ballc@opd.wi.gov
Attorney for the State Public Defender

CERTIFICATION AS TO FORM/LENGTH

I certify that this brief meets the form and length requirements of Rule 809.19(8)(b) and (c) in that it is: proportional serif font, minimum printing resolution of 200 dots per inch, 13 point body text, 11 point for quotes and footnotes, leading of minimum 2 points and maximum of 60 characters per line of body text. The length of the brief is 2,524 words.

CERTIFICATE OF COMPLIANCE WITH RULE 809.19(12)

I hereby certify that I have submitted an electronic copy of this brief, excluding the appendix, if any, which complies with the requirements of § 809.19(12).

I further certify that this electronic brief is identical in content and format to the printed form of the brief filed on or after this date.

This certificate has been attached to the paper copies of this brief filed with the court and served on all opposing parties. The brief is being filed and served by U.S. Mail.

Dated this 13th day of January, 2015.

Signed:

COLLEEN D. BALL
Assistant State Public Defender
State Bar No. 1000729

Office of State Public Defender
735 North Water Street, Suite 912
Milwaukee, WI 53202-4116
(414)227-3110
ballc@opd.wi.gov

Attorney for the State Public Defender