RECEIVED
04-11-2014
CLERK OF COURT OF APPEALS
OF WISCONSIN

STATE OF WISCONSIN

COURT OF APPEALS

DISTRICT I

Appeal No. 2013AP362-CR
(Milwaukee County Cir. Ct. Case No. 2012CF438)

STATE OF WISCONSIN,

Plaintiff-Respondent,

v.

KELLY M. RINDFLEISCH,

Defendant-Appellant.

ON APPEAL FROM AN ORDER DENYING SUPPRESSION AND FROM A JUDGMENT OF CONVICTION ENTERED IN MILWAUKEE COUNTY CIRCUIT COURT, THE HONORABLE DAVID A. HANSHER PRESIDING

BRIEF AND SUPPLEMENTAL APPENDIX OF PLAINTIFF-RESPONDENT STATE OF WISCONSIN

J.B. VAN HOLLEN
Attorney General

CHRISTOPHER G. WREN
Assistant Attorney General
State Bar No. 1013313

Attorneys For Plaintiff-
Respondent State of Wisconsin

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 266-7081
wrencg@doj.state.wi.us

TABLE OF CONTENTS

Page

Questions Presented 1

Position on Oral Argument and Publication of the Court's Opinion 2

Constitutional Provision and Statutes Involved 3

Statement of the Case: Facts and Procedural History 7

Standards of Review 14

A. Grant Or Denial Of Suppression Motion. 14

B. Statutory Interpretation..... 16

C. Exercise Of Discretion. 17

Argument..... 18

I. Removing The Shine From The Shiny Object: For Fourth Amendment Purposes, Electronic Data Does Not Differ Significantly From Conventional Paper-Based Data. 18

II. The Circuit Court Correctly Rejected Rindfleisch's Overbreadth Challenge To The Search Warrants By Which The State Acquired E-mail Messages From Gmail And Yahoo! Accounts Established By Rindfleisch. 24

A. The Warrants Satisfied The Fourth Amendment's Particularity Criterion. 25

B. Rindfleisch's As-Applied Challenge To The Constitutionality Of Wis. Stat. § 968.375 Goes Long On Rhetoric, Short On Analysis and Sense. 36

C. Rindfleisch Makes a Meritless Argument About The Circuit Court's Reference To Rule 41(e)(2)(B) Of The Federal Rules Of Criminal Procedure..... 40

D. Because The Argument By Rindfleisch About The Warrants' Alleged Overbreadth Amounts To A Pared-Down Version Of Her Argument Alleging That The Warrants Lacked Sufficient Particularity, The State Relies On Its Earlier Argument On The Particularity Issue. 45

E. Although This Court Should Hold That The Google And Yahoo! Warrants Complied With The Requirements Of The Fourth Amendment And Article I, Section 11 Of The Wisconsin Constitution, If This Court Concludes The Warrants Did Not Comply, The Court Should Remand The Case To The Circuit Court For An Evidentiary Hearing At Which The State Would Have An Opportunity To Show That The State Obtained Rind-

Page

fleisch's Computer Laptop And Contents As A Result Not Of The Noncompliant Warrants, But Rather "'By Means Sufficiently Distinguishable To Be Purged Of The Primary Taint.'" 46

F. For Fourth Amendment Purposes, Digital Data Does Not Differ From Nondigital Data In Sufficiently Significant Ways To Require Creating New Doctrines For Digital Data. 47

Conclusion 51

Certificate of Compliance with Wis. Stat. § (Rule) 809.19(8): Form and Length Requirements 52

Certificate of Compliance with Wis. Stat. § (Rule) 809.19(12): Electronic Brief..... 53

Certificate of Compliance with Wis. Stat. § (Rule) 809.19(2)(a): Supplemental Appendix 54

TABLE OF AUTHORITIES

CASES

In re Termination of Parental Rights to Gwenevere T., 2011 WI 30, 333 Wis. 2d 273, 797 N.W.2d 854 36

In re 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) 33, 34, 48

Kentucky v. King, 563 U.S. ___, 131 S. Ct. 1849 (2011) 26

Keplin v. Hardware Mut. Cas. Co., 24 Wis. 2d 319, 129 N.W.2d 321 (1964) 31

McNulty v. Reddy Ice Holdings, Inc., 271 F.R.D. 569 (E.D. Mich. 2011) 21

Peplinski v. Fobe's Roofing, Inc., 193 Wis. 2d 6, 531 N.W.2d 597 (1995) 18

Performance Pricing, Inc. v. Google Inc., 2009 WL 2832353 (E.D. Tex. Aug. 31, 2009) 21

Russell v. Harms, 397 F.3d 458 (7th Cir. 2005)..... 27

Sohns v. Jensen, 11 Wis. 2d 449, 105 N.W.2d 818 (1960) 16

State ex rel. Kalal v. Circuit Court for Dane Cnty., 2004 WI 58, 271 Wis. 2d 633, 681 N.W.2d 110 16

Page

State v. Artic,
2010 WI 83, 327 Wis. 2d 392,
786 N.W.2d 430 47

State v. Buchanan,
2013 WI 31, 346 Wis. 2d 735,
828 N.W.2d 847 ..... 16, 17

State v. Burton,
2007 WI App 237, 306 Wis. 2d 403,
743 N.W.2d 152 17

State v. Delgado,
223 Wis. 2d 270, 588 N.W.2d 1
(1999) 17

State v. Dubose,
2005 WI 126, 285 Wis. 2d 143,
699 N.W.2d 582 15

State v. Eason,
2001 WI 98, 245 Wis. 2d 206,
629 N.W.2d 625 15

State v. Keith,
216 Wis. 2d 61, 573 N.W.2d 888
(Ct. App. 1997) 14, 15

State v. King,
187 Wis. 2d 548, 523 N.W.2d 159
(Ct. App. 1994) 15

State v. Leutenegger,
2004 WI App 127, 275 Wis. 2d 512,
685 N.W.2d 536 16

State v. Lonkoski,
2013 WI 30, 346 Wis. 2d 523,
828 N.W.2d 552 15

State v. Owens,
148 Wis. 2d 922, 436 N.W.2d 869
(1989) 15

State v. Poellinger,
153 Wis. 2d 493, 451 N.W.2d 752
(1990) 15

State v. Schroeder,
2000 WI App 128, 237 Wis. 2d 575,
613 N.W.2d 911 33

State v. Turner,
136 Wis. 2d 333, 401 N.W.2d 827
(1987) 16

State v. Wilks,
117 Wis. 2d 495, 345 N.W.2d 498
(Ct. App.) aff'd, 121 Wis. 2d 93, 358
N.W.2d 273 (1984) 16

State v. Ziegler,
2012 WI 73, 342 Wis. 2d 256,
816 N.W.2d 238 17

United States v. Bowen,
689 F. Supp. 2d 675 (S.D.N.Y.
2010) 33, 35, 36

United States v. Brooks,
2014 WL 292194 (M.D. Fla. Jan.
27, 2014) 34

Page

United States v. Burgess,
576 F.3d 1078 (10th Cir. 2009)..... 22

United States v. Carey,
172 F.3d 1268 (10th Cir. 1999)..... 32, 33

United States v. Cioffi,
668 F. Supp. 2d 385 (E.D.N.Y.
2009) 34

United States v. Comprehensive Drug
Testing, Inc.,
579 F.3d 989 (9th Cir. 2009)..... 35

United States v. Conrad,
2013 WL 4028273 (M.D. Fla. Aug.
7, 2013) 22, 34

United States v. Grubbs,
547 U.S. 90 (2006)..... 26, 43

United States v. Kernell,
2010 WL 1491873 (E.D. Tenn. Mar.
31, 2010) 43

United States v. Kernell,
2010 WL 1490921 (E.D. Tenn. Apr.
13, 2010) 43

United States v. Leary,
846 F.2d 592 (10th Cir. 1988)..... 32, 33

United States v. Liu,
239 F.3d 138 (2d Cir. 2000) 36

United States v. Mann,
592 F.3d 779 (7th Cir. 2010)..... 33, 35

United States v. Richards,
659 F.3d 527 (6th Cir. 2011)..... 26, 27

United States v. Roberts,
2010 WL 234719
(E.D. Tenn. Jan. 14, 2010)..... 43

United States v. Schesso,
730 F.3d 1040 (9th Cir. 2013)..... 40

United States v. Stubbs,
873 F.2d 210 (9th Cir. 1989)..... 32

United States v. Taylor,
764 F. Supp. 2d 230 (D. Me. 2011)..... 18, 21, 33,
..... 34, 35

United States v. Tylman,
2007 WL 2669567 (C.D. Ill. Aug.
22, 2007) 44

United States v. Vitek Supply Corp.,
144 F.3d 476 (7th Cir. 1998)..... 33

United States v. White,
416 F.3d 634 (7th Cir. 2005)..... 23

United States v. Widner,
2010 WL 4861513 (W.D.N.Y. Aug.
20, 2010) 42, 43

United States v. Williams,
650 F. Supp. 2d 633 (W.D. Ky.
2009) 40

United States v. Winther,
2011 WL 5837083 (E.D. Pa. Nov.
18, 2011) 41

Page

Wong Sun v. United States,
371 U.S. 471 (1963) 46

STATUTES

U. S. Const. amend. IV 3, 46, 47

Wis. Const. art. I, § 11 ..... 46, 47

Wis. Stat. § 809.19(3)(a)2. 7

Wis. Stat. § 809.23(1)(a)1. 2

Wis. Stat. § 809.23(3)(b) 2

Wis. Stat. § 946.12 3

Wis. Stat. § 946.12(3) 9, 12

Wis. Stat. § 968.375 ..... 4, 36, 37, 38, 39, 44

Wis. Stat. § 968.375(4)(a) 37

LEGISLATION

2009 Wis. Act 329, § 6..... 4

2013 Wis. Act 167, §§ 4-16..... 4

RULES

Fed. R. Crim. P. 41..... 43, 44

Fed. R. Crim. P. 41(e)(2)(A)(i) 42

Fed. R. Crim. P. 41(e)(2)(B) ..... ii, 25, 40, 42, 43, 44

OTHER AUTHORITIES

The American Heritage Dictionary of the English Language (5th ed. 2011) 20

Francis Bacon, The Essays (Scolar Press 1971) (1625)..... 44

Daniel Bice, No Quarter, Walker staffer quits after admitting she posted Web comments while at work, Milwaukee Journal Sentinel, May 14, 2010 8

Black's Law Dictionary (9th ed. 2009)..... 41

Robert Crowston, Hilbert's Hotel, NRICH, http://nrich.maths.org/5788 23

Ralph Losey, Sedona's New Commentary on Search, and the Myth of the Pharaoh's Curse, e-Discovery Team 49

Megabytes, Gigabytes, Terabytes... What Are They?," What's A Byte?, http://www.whatsabyte.com 20

Steven Strogatz, The Hilbert Hotel, N.Y. Times, May 9, 2010 23

Christopher G. Wren & Jill Robinson Wren, Using Computers in Legal Research: A Guide to LEXIS and WESTLAW (1994)..... 50

STATE OF WISCONSIN

COURT OF APPEALS

DISTRICT I

Appeal No. 2013AP362-CR
(Milwaukee County Cir. Ct. Case No. 2012CF438)

STATE OF WISCONSIN,

Plaintiff-Respondent,

v.

KELLY M. RINDFLEISCH,

Defendant-Appellant.

ON APPEAL FROM AN ORDER DENYING SUPPRESSION AND FROM A JUDGMENT OF CONVICTION ENTERED IN MILWAUKEE COUNTY CIRCUIT COURT, THE HONORABLE DAVID A. HANSHER PRESIDING

BRIEF OF PLAINTIFF-RESPONDENT STATE OF WISCONSIN[1]

QUESTIONS PRESENTED

1. For Fourth Amendment purposes, does digital data differ from analog or nondigital data significantly enough to require, for digital data, substantial alterations of Fourth Amendment doctrines developed in the context of nondigital data?

   - The circuit court did not address this issue.
   - This court should answer "No."

---

[1] The electronically filed versions of this brief and separate supplemental appendix include hyperlinked bookmarks intended to facilitate online reading.

2. Did the circuit court properly deny the suppression motion of defendant-appellant Kelly M. Rindfleisch that asserted the invalidity of two warrants because those warrants supposedly failed to satisfy the particularity requirement of the Fourth Amendment?

   - By its decision, the circuit court implicitly answered "Yes."
   - This court should answer "Yes."

3. Did the circuit court properly reject Rindfleisch's claim that the warrants suffered from overbreadth?

   - By its decision, the circuit court implicitly answered "Yes."
   - This court should answer "Yes."

POSITION ON ORAL ARGUMENT AND PUBLICATION OF THE COURT'S OPINION

Oral argument. The State concurs in Rindfleisch's request for oral argument.

Publication. The State recommends publication of the court's opinion. The State believes the court's opinion will provide guidance about and clarify issues regarding the scope of subpoenas and search warrants for electronically stored documents held by entities other than a defendant. *Cf.* Wis. Stat. § (Rule) 809.23(1)(a)1. (the opinion may "[e]nunciate[ ] a new rule of law or . . . clarif[y] . . . an existing rule"). If the court elects not to recommend its opinion for publication, however, the State requests that the court issue the opinion as an authored opinion rather than as a *per curiam* opinion, memorandum opinion, or summary disposition order. Wis. Stat. § (Rule) 809.23(3)(b) (authorizing citation, for per-

suasive value, of unpublished authored opinions issued on or after July 1, 2009).

CONSTITUTIONAL PROVISION AND STATUTES INVOLVED[2]

UNITED STATES CONSTITUTION, AMENDMENT IV.

> 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.

WIS. STAT. § 946.12 MISCONDUCT IN PUBLIC OFFICE.

> **946.12 Misconduct in public office.** Any public officer or public employee who does any of the following is guilty of a Class I felony:
>
> **(1)** Intentionally fails or refuses to perform a known mandatory, nondiscretionary, ministerial duty of the officer's or employee's office or employment within the time or in the manner required by law; or
>
> **(2)** In the officer's or employee's capacity as such officer or employee, does an act which the officer or employee knows is in excess of the officer's or employee's lawful authority or which the officer or employee knows the officer or employee is forbidden by law to do in the officer's or employee's official capacity; or
>
> **(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 oth-

[2] Unless indicated otherwise, all citations to Wisconsin Statutes refer to the 2011-12 edition.

ers and with intent to obtain a dishonest advantage for the officer or employee or another; or

(4) In the officer's or employee's capacity as such officer or employee, makes an entry in an account or record book or return, certificate, report or statement which in a material respect the officer or employee intentionally falsifies; or

(5) Under color of the officer's or employee's office or employment, intentionally solicits or accepts for the performance of any service or duty anything of value which the officer or employee knows is greater or less than is fixed by law.

WIS. STAT. § 968.375 SUBPOENAS AND WARRANTS FOR RECORDS OR COMMUNICATIONS OF CUSTOMERS OF AN ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE PROVIDER.[3]

968.375 Subpoenas and warrants for records or communications of customers of an electronic communication service or remote computing service provider. (2) JURISDICTION. For purposes of this section, a person is considered to be doing business in this state and is subject to service and execution of process from this state, if the person makes a contract with or engages in a terms of service agreement with any other person, whether or not the other person is a resident of this state, and any part of the performance of the contract or provision of service takes place within this state on any occasion.

(3) SUBPOENA. (a) Upon the request of the attorney general or a district attorney and upon a showing of probable cause, a judge may issue a subpoena requiring a person who provides electronic communication service or remote computing service to dis-

[3] Created by 2009 WIS. ACT 349, § 6 (effective May 28, 2010). The legislature recently amended the statute to renumber the subsections and update the internal cross-references. *See* 2013 WIS. ACT 167, §§ 4-16 (effective Mar. 29, 2014). For related federal authorities, see R-Ap. 501-42.

close within a reasonable time that is established in the subpoena a record or other information pertaining to a subscriber or customer of the service, including any of the following relating to the subscriber or customer:

1. Name.

2. Address.

3. Local and long distance telephone connection records, or records of session times and durations.

4. Length of service, including start date, and types of service utilized.

5. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address.

6. Means and source of payment for the electronic communication service or remote computing service, including any credit card or bank account number.

(b) A subpoena under this subsection may not require disclosure of the contents of communications.

(4) WARRANT. Upon the request of the attorney general or a district attorney and upon a showing of probable cause, a judge may issue a warrant requiring a person who provides electronic communication service or remote computing service to disclose within a reasonable time that is established in the warrant any of the following:

(a) The content of a wire or electronic communication that is in electronic storage in an electronic communications system or held or maintained by a provider of remote computing service.

(b) A record or information described under sub. (3) (a).

(5) BASIS, APPLICATION FOR, AND ISSUANCE OF SUBPOENA OR WARRANT. Section 968.12 (2) and (3) applies to the basis and application for, and issuance of, a subpoena under sub. (3) or a warrant under sub. (4) as it applies to the basis and application for, and issuance of, a search warrant under s. 968.12.

(6) MANNER OF SERVICE. A subpoena or warrant issued under this section may be served in the manner provided for serving a summons under s. 801.11 (5) or, if delivery can reasonably be proved, by Unit-

ed States mail, delivery service, telephone facsimile, or electronic transmission.

(7) TIME FOR SERVICE. A subpoena or warrant issued under this section shall be served not more than 5 days after the date of issuance.

(9) MOTION TO QUASH. The person on whom a subpoena or warrant issued under this section is served may file a motion to quash the subpoena or warrant with the judge who issued the subpoena or warrant. If the person files the motion within the time for production of records or information, the judge shall hear and decide the motion within 8 days after the motion is filed.

(10) LAW ENFORCEMENT PRESENCE NOT REQUIRED. The presence of a law enforcement officer is not required for service or execution of a subpoena or warrant issued under this section.

(11) RETURN. A subpoena or warrant issued under this section shall be returned to the court not later than 5 days after the records or information described in the subpoena or warrant are received by the attorney general, district attorney, or law enforcement agency, whichever is designated in the subpoena or warrant.

(12) SECRECY. A subpoena or warrant issued under this section shall be issued with all practicable secrecy and the request, complaint, affidavit, or testimony upon which it is based may not be filed with the clerk or made public until the subpoena or warrant has been executed and returned to the court. The judge may issue an order sealing the subpoena or warrant and the request, complaint, affidavit, or testimony upon which it is based. The judge may issue an order prohibiting the person on whom the subpoena or warrant is served from disclosing the existence of the subpoena or warrant to the customer or subscriber unless the judge subsequently authorizes such disclosure.

(13) IMMUNITY. A person on whom a subpoena or warrant issued under this section is served is immune from civil liability for acts or omissions in providing records or information, facilities, or assistance in accordance with the terms of the subpoena or warrant.

(14) TECHNICAL IRREGULARITIES. Evidence disclosed under a subpoena or warrant issued under this section shall not be suppressed because of technical irregularities or errors not affecting the substantial rights of the defendant.

(15) DISCLOSURE WITHOUT SUBPOENA OR WARRANT. A provider of electronic communication or remote computing service may disclose records or information described under sub. (3) (a) of a customer or subscriber or the content of communications of a customer or subscriber described under sub. (4) without a subpoena or warrant if any of the following applies:

(a) The customer or subscriber provides consent for the particular disclosure.

(b) The provider of electronic communication or remote computing service believes in good faith that an emergency involving the danger of death or serious physical injury to any person exists and that disclosure of the information is required to prevent the death or injury or to mitigate the injury.

STATEMENT OF THE CASE: FACTS AND PROCEDURAL HISTORY

As respondent, the State exercises its option not to present a full statement of the case. Wis. Stat. § (Rule) 809.19(3)(a)2. Instead, the State offers this supplemental statement of facts and will present additional facts in the "Argument" portion of its brief.

This appeal arises from a John Doe proceeding that originally had nothing to do with Kelly Rindfleisch.[4]

---

[4] *In re John Doe Proceeding*, No. 10JD7 (Milwaukee County Cir. Ct.).

On Thursday, May 13, 2012, Darlene Wink, constituent services coordinator for Milwaukee's then-County Executive Scott Walker, resigned 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" (87:Ex. 9, at 4 (Ex. SW41); *see also* 3:4, R-Ap. 107).[5]

On August 11, 2010, Milwaukee County District Attorney Chief Investigator David E. Budde submitted an affidavit (dated August 6, 2010) "in connection with a request for a search warrant for all records and information relating to the investigation of political activity carried on by Darlene Wink in the Office of the Milwaukee County Executive in the Milwaukee County Courthouse, 901 North 9th Street, Milwaukee, WI" (87:Ex. 1, at 1). 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 (an enlargement relating to "blog-posting activity by Darlene Wink as 'rpmcvp' while serving as an employee in the Office of the County Executive" (87:Ex. 1, at 2)) and an affidavit dated July 1, 2010 "in support of a Search Warrant for the Yahoo Mail accounts of Darlene Wink" (87:Ex. 1, at 2). "Both of these Affidavits tend to establish that Darlene Wink conducted partisan political activity while engaged in her official position as an employee within the Office of the Milwaukee County

---

[5] Daniel Bice, No Quarter, *Walker staffer quits after admitting she posted Web comments while at work*, MILWAUKEE JOURNAL SENTINEL, May 14, 2010, http://www.jsonline.com/watchdog/noquarter/93746099.html (last visited Apr. 10, 2014).

Executive" (87:Ex. 1, at 2). Investigator Budde's affidavit went on to assert that

> based upon new information obtained in large part – if not exclusively – through the process issued in the John Doe investigation, I have discovered additional evidence that Darlene Wink appears to have been engaged in substantial political activity on multiple occasions over a sustained period of time while she was working as an employee in the offices of the Milwaukee County Executive.

(87:Ex. 1, at 2.) Neither the affidavit nor the accompanying exhibits implicated Rindfleisch in any violation of Wis. Stat. § 946.12(3), which prohibits misconduct in public office (see p. 3, above).

On August 16, 2010, Investigator Budde submitted an affidavit (dated August 12, 2010) "in connection with a request for multiple search warrants, all relating to the investigation of political activity carried on by Darlene Wink in the Office of the Milwaukee County Executive" (87:Ex. 2, at 1). The warrants identified "records and information" (*i.e.*, e-mails) relating to several individuals[6] as the objects of the warrants (87:Ex. 2, at 5-7). Neither the affidavit nor the accompanying exhibits implicated Rindfleisch in any violation of section 946.12(3).

On August 20, 2010, Investigator Budde submitted an affidavit (dated August 20, 2010) in support of a search-warrant application "principally to search and seize records and information in

---

[6] The affidavit identified the individuals as Tim Russell, Joe Fadness, Rose Ann Dieck, Fran McLaughlin, Herb Ripka, David Karst, and Doug Haag (87:Ex. 2, at 1-2, 4-5, 6).

the form of digital evidence contained on computer workstations issued by Milwaukee County for Tim Russell's use" (87:Ex. 4, at 1). Investigator Budde asserted that he had "discovered evidence that Tim Russell was engaged in political activity on multiple occasions over a sustained period of time while he was working as an employee in the Office of the Milwaukee County Executive and … as an Administrator for the Department of Health and Human Services (DHHS)" (87:Ex. 4, at 1). The affidavit did not refer to Rindfleisch (87:Ex. 4, at 1-9), although one affidavit exhibit — "e-mails demonstrat[ing] partisan political activity during periods of time when Russell was acting as a Milwaukee County employee" (87:Ex. 4, at 4) — included Rindfleisch's e-mail addresses in either the "To" or "From" line in e-mail headers (87:Ex. 4, at Ex. D).

On October 20, 2010, Investigator Budde submitted an affidavit (dated October 19, 2010) in support of a search-warrant application to "require the production of e-mails from e-mails accounts" (87:Ex. 6, at 1, R-Ap. 276) at Google and Yahoo! by several individuals and a political entity: Tim Russell, Kelly Rindfleisch, Brian Pierick, and ScottForGov (87:Ex. 6, at 3-6, R-Ap. 278-81). Investigator Budde

> request[ed] that the Court issue warrants to search the [Google and Yahoo!] premises for all records and information relation to violations of Wisconsin Statute §946.12, viz. Misconduct in Public Office, for the time period since January 1, 2009. I submit that this time period is reasonably related to the current campaign season for the Office of the Governor.

(87:Ex. 6, at 6, R-Ap. 281.) The affidavit identified the objects of the search as including "Gmail records and information associated with the sub-

scriber ID[ ] … kmrindfleisch@gmail.com" (87:Ex. 6, at 6, R-Ap. 281) and "Yahoo! records and information associated with the subscriber ID[ ] … rellyk_us@yahoo.com" (87:Ex. 6, at 7, R-Ap. 282). Investigator Budde "ask[ed] that the court authorize the search of the[ ] additional e-mail accounts identified above because I believe they will contain evidence Misconduct in Public Office. I submit that this evidence will be both relevant and valuable in this investigation for the following reasons" (87:Ex. 6, at 12, R-Ap. 287). He "submit[ted] that … rellyk_us@yahoo.com and kmrindfleisch@gmail .com[ ] will contain evidence of Tim Russell's misconduct" (87:Ex. 6, at 12, R-Ap. 287). Investigator Budde explained:

> a. These e-mail records will corroborate other existing e-mail evidence in this case;
>
> b. While e-mail accounts will often contain many e-mails dating back over months or even years, it is entirely probable that (as I am advised by IT Manager Jim Krueger) over time a user can delete "without a trace" some e-mail held in accounts that are hosted by a provider of electronic communication services. That is to say that e-mails may not be found in timrussellwi@ gmail.com because they have been deleted, but such e-mails may remain in the Rindfleisch.
>
> c. A review of the e-mail threads in this investigation suggest that a number of potentially relevant e-mails have been deleted from the tim russellwi 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 email accounts will be relevant and valuable.

(87:Ex. 6, at 12-13, R-Ap. 287-88.)

In response to the warrants, the John Doe prosecutor received "a CD from Google which contained a Gmail for Kelly Rindfleisch that had been previously subpoenaed in this John Doe" relating to the kmrindfleisch@gmail.com account (87:Ex. 9 (hr'g tr.), at 11-12, R-Ap. 325-26). Based on a review of those e-mails, Investigator Budde had "reason to believe that the deputy chief of staff [Rindfleisch] was active in fund-raising in the County Executive's Office in the last ten months" (87:Ex. 9 (hr'g tr.), at 12, R-Ap. 326).

At the hearing to expand the John Doe proceeding and to establish probable cause for warrants to search the County Executive's office and Rindfleisch's automobile and two residences (87:Ex. 9 (hr'g tr.), at 3-4, 7-8, R-Ap. 317-18, 321-22), Investigator Budde reviewed a dozen e-mails sent on county time by Rindfleisch relating to political activity, including fundraising (87:Ex. 9 (hr'g tr.), at 12-35, R-Ap. 326-49 (identifying and explaining exhibits SW-1 through SW-12)). The court granted the request to enlarge the scope of the John Doe proceeding and granted the search-warrant requests (87:Ex. 9 (hr'g tr.), at 103-14, R-Ap. 417-28).

On January 26, 2012, the Milwaukee County District Attorney's office charged Rindfleisch with four counts of misconduct in public office, each a Class I felony and each a violation of section 946.12(3)[7] (3:1, R-Ap. 104). The complaint identified Rindfleisch's activities underlying the charges (3:13, 15-50, R-Ap. 116, 118-53) and provided de-

---

[7] *See supra* p. 3.

tails about the secret wireless networking system used for those activities (3:3, 14-15, 50, R-Ap. 106, 117-18, 153).[8]

On June 26, 2012, Rindfleisch filed a motion "for an order suppressing all evidence obtained by the state via search warrants issued on October 20, 2010, seeking information from Rindfleisch's Yahoo and Gmail accounts" (23, R-Ap. 165) Rindfleisch contended that "[t]he warrant application and affidavit in this case, and the warrant itself, fail to establish probable cause that all of the information the state sought constituted evidence of any crime or evidence, and if so, what" (24:6, R-Ap. 171), and that "section 968.375 is unconstitutional as applied in this case" (24:9, R-Ap. 174). The motion included copies of the two warrants (26:2-4, 6-8, R-Ap. 180-82, 184-86) and copies of judicial decisions purportedly supporting Rindfleisch's contentions (26:10-254; *see also* 26:10, 23, 70, 78, 109, 114, 126, 144, 155, 177, 194, 201, 217, 220, 228, 233, 240, 249, R-Ap. 188-205 (first pages of decisions)). The State responded with a brief (36, R-Ap. 206-15) and exhibits (37:3, 15, 25, 33, 45-48, R-Ap. 218-25). Rindfleisch filed a reply (40, R-Ap. 226-37), to which the State filed a rejoinder (41, R-Ap. 238-39).

On August 21, 2012, the circuit court held a hearing at which the court orally denied the suppression motion (83, R-Ap. 442-52). On September

---

[8] At the change-of-plea hearing, Rindfleisch and her lawyer did not dispute the facts in the criminal complaint (84:15, R-Ap. 466) and stipulated to those facts (with one exception not applicable here) as establishing the factual basis for Rindfleisch's plea (84:19-20, R-Ap. 471-72).

14, 2012, the court entered a written order confirming the oral decision (51, R-Ap. 101).

On October 11, 2012, Rindfleisch entered a guilty plea to Count One of the criminal complaint (84:14, R-Ap. 466; *see also* 3:1, R-Ap. 104; 73, R-Ap. 245-54 (plea questionnaire)).

On November 19, 2010, the circuit court sentenced Rindfleisch to three years' imprisonment, stayed the sentence, and placed her on probation for three years (78:1, R-Ap. 102). The court imposed six months of confinement (with Huber work-release privileges) in the Milwaukee County House of Correction as a condition of probation (78:1, R-Ap. 102). The court stayed the jail time pending appeal (78:1, R-Ap. 102).

This appeal followed.

STANDARDS OF REVIEW

A. Grant Or Denial Of Suppression Motion.

Whether to grant or deny a motion to suppress evidence lies within the discretion of the circuit court. ***State v. Keith***, 216 Wis. 2d 61, 68, 573 N.W.2d 888 (Ct. App. 1997). Therefore, an appellate court will overturn an evidentiary decision of the circuit court only if that court erroneously exercised its discretion. ***Id.*** at 69.

> When we review a discretionary decision, we examine the record to determine if the circuit court logically interpreted the facts, applied the proper legal standard, and used a demonstrated rational process to reach a conclusion that a reasonable judge could reach. In considering whether the proper legal standard was applied, however, no deference is due. This court's function is to correct legal errors. There-

> fore, we review *de novo* whether the evidence before the circuit court was legally sufficient to support its rulings. Furthermore, if evidence has been erroneously admitted or excluded, we will independently determine whether that error was harmless or prejudicial.

Id. (citations omitted). *See also* ***State v. Eason***, 2001 WI 98, ¶ 9, 245 Wis. 2d 206, 629 N.W.2d 625.

> On review of a motion to suppress, [an appellate] court employs a two-step analysis. 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. . . . 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 analyses of the circuit court . . . .

State v. Dubose, 2005 WI 126, ¶ 16, 285 Wis. 2d 143, 699 N.W.2d 582 (citations omitted). *See also* ***State v. Lonkoski***, 2013 WI 30, ¶ 21, 346 Wis. 2d 523, 828 N.W.2d 552; ***State v. Poellinger***, 153 Wis. 2d 493, 506-07, 451 N.W.2d 752 (1990) ("[W]hen faced with a record of historical facts which supports more than one inference, an appellate court must accept and follow the inference drawn by the trier of fact unless the evidence on which that inference is based is incredible as a matter of law.");[9] ***State v. Owens***, 148 Wis. 2d 922, 929-30, 436 N.W.2d 869 (1989) (when an appellate court reviews a circuit court's decision on a

---

[9] "[']Incredible as a matter of law['] means inherently incredible, such as in conflict with the uniform course of nature or with fully established or conceded facts." ***State v. King***, 187 Wis. 2d 548, 562, 523 N.W.2d 159 (Ct. App. 1994) (citations omitted).

suppression motion, the appellate court defers to the circuit court's credibility determinations); ***State v. Turner***, 136 Wis. 2d 333, 343-44, 401 N.W.2d 827 (1987) (appellate court will sustain "the trial court's findings of historical or evidentiary fact unless they are contrary to the great weight and clear preponderance of the evidence. This is basically a 'clearly erroneous' standard of review.").

"[W]here a trial court does not expressly make a finding necessary to support its legal conclusion, an appellate court can assume that the trial court made the finding in the way that supports its decision." ***State v. Wilks,*** 117 Wis. 2d 495, 503, 345 N.W.2d 498 (Ct. App.), *aff'd*, 121 Wis. 2d 93, 358 N.W.2d 273 (1984). Thus, "[a]ppellate courts may assume facts, reasonably inferable from the record, in a manner that supports the trial judge's decision." ***State v. Leutenegger***, 2004 WI App 127, ¶ 30 n.7, 275 Wis. 2d 512, 685 N.W.2d 536. *See also* ***Sohns v. Jensen***, 11 Wis. 2d 449, 453, 105 N.W.2d 818 (1960) ("The court on appeal will also assume when a finding is not made on an issue which appears from the record to exist, that it was determined in favor of or in support of the judgment.").

B. Statutory Interpretation.

"Interpretation of a statute is a question of law that [an appellate] court reviews de novo while benefitting from the analyses of the lower courts." ***State v. Buchanan***, 2013 WI 31, ¶ 12, 346 Wis. 2d 735, 828 N.W.2d 847. Statutory interpretation "'begins with the language of the statute.'" ***State ex rel. Kalal v. Circuit Court for Dane Cnty.***, 2004 WI 58, ¶ 45, 271 Wis. 2d 633, 681 N.W.2d 110. "'The purpose of statutory interpreta-

tion is to determine what the statute means so that it may be given its full, proper, and intended effect.'" ***State v. Ziegler***, 2012 WI 73, ¶ 42, 342 Wis. 2d 256, 816 N.W.2d 238 (quoted source omitted). An appellate court "must construe statutory language reasonably; an unreasonable interpretation is one that yields absurd results or one that contravenes the statute's manifest purpose." ***Buchanan***, 346 Wis. 2d 735, ¶ 23; *see also* ***Ziegler***, 342 Wis. 2d 256, ¶ 43.

C. Exercise Of Discretion.

> Evidentiary determinations are within the trial court's broad discretion and will be reversed only if the trial court's determination represents a prejudicial misuse of discretion. [An appellate court] will find an erroneous exercise of discretion where a trial court failed to exercise discretion, the facts fail to support the decision, or the trial court applied the wrong legal standard.

State v. Burton, 2007 WI App 237, ¶ 13, 306 Wis. 2d 403, 743 N.W.2d 152 (citations omitted).

> The term "discretion" contemplates a process of reasoning which depends on facts in the record or reasonably derived by inference from the record that yield a conclusion based on logic and founded on proper legal standards. The record on appeal must reflect the circuit court's reasoned application of the appropriate legal standard to the relevant facts of the case.

State v. Delgado, 223 Wis. 2d 270, 280-81, 588 N.W.2d 1 (1999) (citations omitted).

> Under this standard, the circuit court's determination will be upheld on appeal if it is a reasonable conclusion, based upon a consideration of the appropriate law and facts of record. . . . While the basis for an exercise of discretion should be set forth in the record, it will be upheld if the appellate court can

> find facts of record which would support the circuit court's decision.

Peplinski v. Fobe's Roofing, Inc., 193 Wis. 2d 6, 20, 531 N.W.2d 597 (1995) (citations omitted).

ARGUMENT

Rindfleisch's appeal rests on a basic assumption: the warrants by which the State obtained e-mail records from Google and Yahoo! suffered from overbreadth. Based on that assumption, Rindfleisch contends that the circuit court erred by denying her motion to suppress the e-mail records and (as derivative evidence) the personal laptop computer seized during the execution of the search warrant at the Milwaukee County Executive's office.

For the reasons that follow, this court should reject Rindfleisch's attack on the Google and Yahoo! warrants and should affirm the judgment of conviction.

I. REMOVING THE SHINE FROM THE SHINY OBJECT: FOR FOURTH AMENDMENT PURPOSES, ELECTRONIC DATA DOES NOT DIFFER SIGNIFICANTLY FROM CONVENTIONAL PAPER-BASED DATA.

Too frequently, judges and litigants seem dazzled when confronted by computer-stored data. This case illustrates the point. Ignoring salient differences from her case, Rindfleisch points to the use of a so-called "filter agent" in ***United States v. Taylor***, 764 F. Supp. 2d 230 (D. Me. 2011), to review a defendant's e-mails to "cull out any potentially privileged materials before either the in-

vestigating agent or prosecutor received them." Rindfleisch's Brief at 23-24.[10] Rindfleisch's reliance on a "filter agent" protocol appears to rest on the character of the seized materials as digital rather than nondigital or analog (*i.e.*, paper-based): Rindfleisch does not appear to contend (or even imply) that an identical warrant for paper-based documents matching the criteria set out in the warrant and supporting affidavit would have implicated any need for a "filter agent."

For Fourth Amendment purposes, whatever differences distinguish digital data from nondigital data do not matter in this case. The size of a data file does not create a distinction for Fourth Amendment purposes. For example, the transcript of the hearing at which the John Doe court enlarged the scope of the John Doe proceeding to include Rindfleisch as a target (87:Ex. 9 (hr'g tr.), R-Ap. 315-441) consists of 127 physical pages measuring 8.5 inches by 11 inches. As the table below shows, the size of a PDF digital version of that document can vary by a factor of eighteen

---

[10] *See also* letter from Franklyn M. Gimbel, counsel for Kelly Rindfleisch, to Judge Patricia S. Curley (Feb. 7, 2014):

> The state's unilateral review of Ms. Rindfleisch's emails, without use of a filter agent and without any effort to protect privileged information, eviscerated her privacy rights under the United States Constitution and the Wisconsin Constitution. The Court's order directing her to conduct the review that should have been conducted by a filter agent years ago provides her such limited relief that she cannot justify the time or expense of such an exercise.

(R-Ap. 494.)

(from 1.08 MB to 19.5 MB), depending on such things as the original scanning resolution and the subsequent processing the file undergoes. Yet, despite this wide variation in digital size, each file contains the same content and number of digital pages as the original paper-based document.

SCAN RESOLUTION OF TRANSCRIPT (IN DOTS PER INCH (DPI))	DIGITAL SIZE (RAW) (IN MEGABYTES (MB))	DIGITAL SIZE (AFTER OCR AND SIZE REDUCTION, *I.E.*, COMPRESSION)
300 dpi	7.36 MB (7,713,657 bytes)	2.61 MB (2,735,231 bytes)
600 dpi	19.5 MB (20,495,036 bytes)	1.08 MB 1,132,835 bytes)

Similarly, digital data does not necessarily equate with an unduly burdensome quantity of data. Here, the response to the Google warrant yielded PDF files totaling a bit less than 218.52 MB (229,138,489 bytes),[11] amounting to 16,168 e-mail pages (87:Ex. 11 (Google search-warrant return)), or slightly more than thirty-two reams of standard 8.5-inch by 11-inch paper, which (for standard 20-pound photocopy paper) would occupy a bit less than five feet five inches of file-cabinet space — not a trivial quantity, but hardly an unmanageable quantity in a legal system where dis-

[11] "Byte" refers to "[a] unit of data equal to eight bits." THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 256 (5th ed. 2011). In this context, "bit" means "[a] binary digit, having either a value of 0 or 1, used to store or represent data." *Id.* at 188 (noting the term's derivation from "b(inary dig)it"). A megabyte (commonly characterized as a million bytes) equals 1,048,576 (or 2^{20}) bytes. *Id.* at 1094. *See also* "Megabytes, Gigabytes, Terabytes... What Are They?," WHAT'S A BYTE?, http://www.whatsabyte.com (last visited Apr. 10, 2014).

covery can run into millions of paper-based pages.[12]

Intermingling of different kinds of files does not distinguish digital data from nondigital data. A paper-based file cabinet can contain a variety of file types — printed documents, photographs, even digital files stored on a CD or DVD —haphazardly filed. Likewise, a computer disk, USB drive, or other electronic-storage device can contain a variety of file types — text, image, audio, video — haphazardly filed.

Intermingling of files with varying degrees of recognized confidentiality or privilege (ranging from none to constitutionally based) does not distinguish digital data from nondigital data.[13] Even in a paper-based filing system, confidential and nonconfidential documents can reside in the same folder (*e.g.*, a physician's report sitting next to a printout of a Wikipedia article on an ailment, or a lawyer's letter of legal advice sitting next to a printout of the lawyer's profile from the lawyer's website).

---

[12] *E.g.*, ***McNulty v. Reddy Ice Holdings, Inc.***, 271 F.R.D. 569, 570 & n.1 (E.D. Mich. 2011) (paper documents totaling approximately 2,600,000 pages and digital data totaling approximately four terabytes (*i.e.*, four trillion bytes), the equivalent of about 880 million pages); ***Performance Pricing, Inc. v. Google Inc.***, 2009 WL 2832353, at *2 (E.D. Tex. Aug. 31, 2009) (1.8 million pages of documents produced).

[13] ***United States v. Taylor***, 764 F. Supp. 2d 230, 235 n.22 (D. Me. 2011) (noting similarity of intermingling in digital and paper-based data).

The need to open a digital file to determine its content does not distinguish digital data from nondigital data. The content of a paper document does not self-disclose; someone must view and at least skim the document to determine (at least preliminarily) its content.[14] Whether confronted by a digital file on a computer disk or a paper document lying face-down on a surface, someone must open it — by invoking a decrypting program like Microsoft Word or by turning the document face up — in order to determine the content of the file or document and thus the relevance of the file or document.

The data container does not distinguish digital data from nondigital data. For example, Google's Gmail service corresponds to a massive brick-and-

---

[14] *Cf.* ***United States v. Conrad***, 2013 WL 4028273 (M.D. Fla. Aug. 7, 2013):

> The warrant was not unconstitutionally overbroad because non-contraband items contained within the computer (such as bank statements, professional records, personal photographs and music) were also subject to seizure. Again, federal courts have consistently recognized that computer searches pose unique challenges that may result in "some innocuous documents [being] examined, at least cursorily in order to determine whether they are, in fact, among those papers authorized to be seized." *Andersen* [*sic*] *v. Maryland*, 427 U.S. 463, 482 n. 11, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976).

Id. at *9. *See also* ***United States v. Burgess***, 576 F.3d 1078, 1094 (10th Cir. 2009) ("[I]n the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files.").

mortar warehouse,[15] with a Gmail customer's e-mail account corresponding to a tenant's storage space in the warehouse. Unless law enforcement officers have reason to believe evidence of a brick-and-mortar tenant's criminal conduct had gotten stored in other tenants' storage spaces in the warehouse, the officers would confine the scope of a search warrant to a "data container" consisting of the target tenant's storage space,[16] which could — likely would — hold "data" of various kinds. Similarly, unless law enforcement officers had reason to believe evidence of a digital tenant's criminal conduct had gotten stored in other digital tenants' storage spaces in the warehouse, the officers would confine the scope of a search warrant to a "data container" consisting of the target tenant's storage space (*e.g.*, an e-mail account), which could hold data of various kinds.

---

[15] Unlike the brick-and-mortar warehouse, however, a digital service like Gmail can quickly expand as necessary to accommodate as many customers as choose to use the service. In effect, a digital service that allocates space for as many customers as arrive at the service's digital doorstep functions much like Hilbert's infinite-rooms hotel. For brief explanations of Hilbert's hotel, see Robert Crowston, *Hilbert's Hotel*, NRICH, http://nrich.maths.org/5788 (last visited Apr. 10, 2014); Steven Strogatz, *The Hilbert Hotel*, N.Y. TIMES, May 9, 2010, http://opinionator.blogs.nytimes.com/2010/05/09/the-hilbert-hotel (last visited Apr. 10, 2014). Regardless of the overall size of the e-mail "warehouse," a customer (through an e-mail account) occupies a specifically identifiable digital storage space.

[16] "When a search involves a building with multiple, separate units, the warrant must specify the precise unit that is the subject of the search to satisfy the particularity requirement." ***United States v. White***, 416 F.3d 634, 637 (7th Cir. 2005).

Ultimately, for Fourth Amendment purposes, the rise of digital data does not require the creation of new doctrines for analyzing the constitutionality of a digital-data search, whether warrantless or pursuant to a warrant. The Fourth Amendment-salient characteristics of digital data readily map to the Fourth Amendment-salient characteristics of nondigital data. In short, digital data do not shine more brightly in the glare of the Fourth Amendment than do nondigital data.

II. THE CIRCUIT COURT CORRECTLY REJECTED RINDFLEISCH'S OVERBREADTH CHALLENGE TO THE SEARCH WARRANTS BY WHICH THE STATE ACQUIRED E-MAIL MESSAGES FROM GMAIL AND YAHOO! ACCOUNTS ESTABLISHED BY RINDFLEISCH.

In the supporting memorandum (24, R-Ap. 166-76) accompanying her suppression motion (23, R-Ap. 165), Rindfleisch referred to "discovery provided to defense counsel" that (in her characterization) showed that "the state sought and obtained *general investigative search warrants* to collect information and evidence from out-of-state internet service providers (ISPs), including Yahoo and Gmail" (24:2, R-Ap. 167 (emphasis added)). She contended that the warrants "failed to identify the objects to be seized with requisite particularity" (24:5, R-Ap. 170) and that "section 968.375 is unconstitutional as applied in this case" (24:9, R-Ap. 174).

On appeal, she reiterates and amplifies those contentions:

- "The Warrants Issued To Yahoo And GMail Lack The Level Of Particularity Required To

Pass Constitutional Muster" (Rindfleisch's Brief at 17).

- "The Circuit Court Misapplied *Bowen*, *Taylor* and *Mann*" (*id.* at 20).
- "The Circuit Court Ignored The *Cunnius* Decision" (*id.* at 26).
- "Section 968.375 Is Unconstitutional As Applied In This Case" (*id.* at 32).
- "The Seizure And Copying Provision Of Rule 41(e)(2)(B) Does Not Trump The Fourth Amendment" (*id.* at 34).
- "The Warrants Were Overbroad" (*id.* at 37).
- "The State Provided No Indicia That The Seizure And Search Of Rindfleisch's Personal Laptop Computer Comported With The Fourth Amendment" (*id.* at 38).
- "Continuing Advances In Technology Mandate Evolving Considerations Of The Fourth Amendment To Protect Citizens As A Matter Of Public Policy" (*id.* at 40).

Rindfleisch's contentions lack merit. This court should reject them and should affirm the judgment of conviction.

A. The Warrants Satisfied The Fourth Amendment's Particularity Criterion.

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.

U.S. Const. amend. IV. "The text of the Amendment thus expressly imposes two requirements. First, all searches and seizures must be reasonable. Second, a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." ***Kentucky v. King***, 563 U.S. ___, 131 S. Ct. 1849, 1856 (2011).

> The Fourth Amendment, however, does not set forth some general "particularity requirement." It specifies only two matters that must be "particularly describ[ed]" in the warrant: "the place to be searched" and "the persons or things to be seized." We have previously rejected efforts to expand the scope of this provision to embrace unenumerated matters. . . . "Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed."

United States v. Grubbs, 547 U.S. 90, 98 (2006) (citations omitted).

> The particularity requirement may be satisfied through the express incorporation or cross-referencing of a supporting affidavit that describes the items to be seized, even though the search warrant contains no such description. "[T]he degree of specificity required is flexible and will vary depending on the crime involved and the types of items sought."

United States v. Richards, 659 F.3d 527, 537 (6th Cir. 2011). "'Although the [F]ourth [A]mendment requires that a search warrant describe the objects of the search with reasonable specificity, it need not be elaborately detailed.'" ***Russell v. Harms***, 397 F.3d 458, 464 (7th Cir. 2005) (citation omitted). "'If detailed particularity is impossible,

generic language is permissible if it particularizes the types of items to be seized.'" ***Id.*** "Applying a reasonableness analysis on a case-by-case basis, the federal courts have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers." ***Richards***, 659 F.3d at 539 (collecting cases).

Despite Rindfleisch's laments, the warrants here satisfied the Fourth Amendment's particularity requirement. The following table summarizes the characteristics of the warrants and supporting affidavit:

CATEGORY OF WARRANT CONTENT	GMAIL WARRANT (26:6-7, R-AP. 184-85) (filed Oct. 20, 2010)	YAHOO! WARRANT (26:2-3, R-AP. 180-81) (filed Oct. 20, 2010)
Incorporation by reference	"attached affidavit [87:Ex 6, R-Ap. 276-308]"	"attached affidavit [87:Ex 6, R-Ap. 276-308]"
Container	"an account identified as kmrindfleisch@gmail.com"	"the account identified as rellyk us@yahoo.com"
Location	"stored at premises owned, maintained, controlled, or operated by Gmail (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA, 94043"	"stored at premises owned, maintained, controlled, or operated by Yahoo, Inc., a company headquartered at 701 First Avenue, Sunnyvale, California 94089"
Period covered	"For the time period of January 1, 2009 to the present"	"For the time period of January 1, 2009 to the present"

CATEGORY OF WARRANT CONTENT	GMAIL WARRANT (26:6-7, R-AP. 184-85) (filed Oct. 20, 2010)	YAHOO! WARRANT (26:2-3, R-AP. 180-81) (filed Oct. 20, 2010)
Reason for period covered	"this time period is reasonably related to the current campaign season for the Office of the Governor" (87:Ex. 6, at 6, R-Ap. 281)	Same
Specified offenses	"violations of Wisconsin Statutes § 946.12, viz., Misconduct in Public Office, by Milwaukee County employee Timothy Russell of the Department of Health and Human Services (and formerly of the Milwaukee County Executive's Office)" (87:Ex. 6, at 1, R-Ap. 276); "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" (26:6, R-Ap. 184)	"violations of Wisconsin Statutes § 946.12, viz., Misconduct in Public Office, by Milwaukee County employee Timothy Russell of the Department of Health and Human Services (and formerly of the Milwaukee County Executive's Office)" (87:Ex. 6, at 1, R-Ap. 276); "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" (26:2, R-Ap. 180)
Records to produce	See ¶¶ (a) through (d) under "Records To Be Produced"	See ¶¶ (a) through (c) under "Records To Be Produced"

CATEGORY OF WARRANT CONTENT	GMAIL WARRANT (26:6-7, R-AP. 184-85) (filed Oct. 20, 2010)	YAHOO! WARRANT (26:2-3, R-AP. 180-81) (filed Oct. 20, 2010)
Objects of search	"all records relating to [specified offenses], 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"	"all records relating to [specified offenses], 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."
Definitions	"'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"; *see also* 87:Ex. 7, at 1, R-Ap. 309.	"'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"; *see also* 87:Ex. 7, at 1, R-Ap. 309.
Purpose	"[Investigator David E. Budde] submit[s] that these Rindfleisch accounts, rellyk_us@yahoo.com and kmrindfleisch@gmail.com, will contain evidence of Tim Russell's misconduct for the fol-	Same

CATEGORY OF WARRANT CONTENT	GMAIL WARRANT (26:6-7, R-AP. 184-85) (filed Oct. 20, 2010)	YAHOO! WARRANT (26:2-3, R-AP. 180-81) (filed Oct. 20, 2010)
	lowing reasons: "a. These e-mail records will corroborate other existing e-mail evidence in this case; "b. While e-mail accounts will often contain many e-mails dating back over months or even years, it is entirely probable that (as I am advised by IT Manager Jim Krueger) over time a user can delete 'without a trace' some e-mail held in accounts that are hosted by a provider of electronic communication services. That is to say that e-mails may not be found in timrussellwi@gmail.com because they have been deleted, but such e-mails may remain in the Rindfleisch. "c. 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	

CATEGORY OF WARRANT CONTENT	GMAIL WARRANT (26:6-7, R-AP. 184-85) (filed Oct. 20, 2010)	YAHOO! WARRANT (26:2-3, R-AP. 180-81) (filed Oct. 20, 2010)
	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 email accounts will be relevant and valuable." (87:Ex. 6, at 12-13, R-Ap. 287-88)	

In her appellate brief, Rindfleisch offers rhetoric but no authority supporting her broad claim the warrants lacked constitutionally sufficient particularity. She writes: "The affidavits in support of the search warrants failed to provide probable cause for the seizure of any and all communications associated with the nominated email accounts regardless of any relationship of those communications to the state's investigation. The warrants permitted the seizure of all communications without any limitation whatsoever." Rindfleisch's Brief at 18.[17]

---

[17] When Rindfleisch filed her brief, the appellate record did not contain the affidavit supporting the warrants. Consequently, she made factual assertions this court could not verify in the appellate record. ***Keplin v. Hardware Mut. Cas. Co.***, 24 Wis. 2d 319, 326, 129 N.W.2d 321 (1964)

(footnote continues on next page)

Nonsense.

Rindfleisch rests her contention on three cases: ***United States v. Stubbs***, 873 F.2d 210 (9th Cir. 1989); ***United States v. Leary***, 846 F.2d 592 (10th Cir. 1988); and ***United States v. Carey***, 172 F.3d 1268 (10th Cir. 1999). Those cases do not aid her. In ***Stubbs***, the warrant "*contained no reference to any criminal activity*. The warrant merely described broad classes of documents without specific description of the items to be seized." ***Stubbs***, 873 F.2d at 212 (emphasis added). The warrant also sought records for a seven-year period. ***Id.*** In addition, "[t]he affidavit filed in support of the warrant [did] not cure the deficiency because the affidavit was neither attached to the warrant nor incorporated by reference." ***Id.*** at 212-13. Even a superficial examination of the warrants in this case shows they did not suffer the deficiencies of the ***Stubbs*** warrant.

In ***Leary***, 846 F.2d 592, the court held that the two limitations[18] in the warrant "provide[d] no limitation at all. The warrant authorize[d], and the customs agents conducted, a general search of

---

(footnote continues from previous page)

(appellate court "cannot consider facts outside the record even though stated as such in the briefs"). The affidavit entered the record as a result of the State's motion to supplement the record.

[18] "First, the documents to be seized had to fall within a long list of business records typical of the documents kept by an export company. Second, those documents had to relate to 'the purchase, sale and illegal exportation of materials in violation of the' federal export laws." ***United States v. Leary***, 846 F.2d 592, 600-01 (10th Cir. 1988).

the Kleinberg offices." ***Id.*** at 601. The court declared the warrant facially overbroad. ***Id.*** Comparing the warrant in ***Leary*** to the warrants in this case shows the pointlessness of Rindfleisch's reliance on ***Leary***: the warrants in this case would have easily survived the challenge mounted in ***Leary***. Notably, in dealing with a warrant far broader than those in Rindfleisch's case, the Seventh Circuit rejected the defendant's reliance on ***Leary***. *See* ***United States v. Vitek Supply Corp.***, 144 F.3d 476, 480-82 (7th Cir. 1998).

Rindfleisch flatly misrepresents ***Carey***, 172 F.3d 1268. Suppression occurred because the search of the computer files exceeded the scope of an otherwise valid warrant as well as the scope of the defendant's consent, resulting in "an unconstitutional general search" of files not included within the scope of the warrant and consent. ***Id.*** at 1276. The court went on, however, to write that "we are quick to note these results are predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result." ***Id.***[19]

Rindfleisch complains that the circuit court misapplied three cases — ***United States v. Mann***, 592 F.3d 779 (7th Cir. 2010); ***Taylor***, 764 F. Supp. 2d 230; and ***United States v. Bowen***, 689 F. Supp. 2d 675 (S.D.N.Y. 2010) — and ignored ***In re the United States of America's Application for a Search Warrant to Seize and Search Electronic Devices from Edward***

---

[19] In ***State v. Schroeder***, 2000 WI App 128, ¶ 16, 237 Wis. 2d 575, 613 N.W.2d 911, this court distinguished ***Carey*** and reached a result different from that in ***Carey***.

Cunnius, 770 F. Supp. 2d 1138 (W.D. Wash. 2011). Rindfleisch's Brief at 20-32. She also relies on ***United States v. Cioffi***, 668 F. Supp. 2d 385 (E.D.N.Y. 2009). Rindfleisch's Brief at 21-22.

Again, Rindfleisch offers a meritless argument. As to ***Cunnius***, 770 F. Supp. 2d 1138, only two cases have cited it, and both rejected its reasoning about the need for a so-called "filter agent" and a promise not to rely on the plain-view doctrine. *See* ***United States v. Brooks***, 2014 WL 292194, at *12 n.19 (M.D. Fla. Jan. 27, 2014) ("In light of the case law previously cited, in which the overwhelming majority of courts have upheld search warrants similar to the one in this case, the undersigned declines to follow the reasoning in *In re United States of America's Application*."); ***United States v. Conrad***, 2013 WL 4028273, at *8 n.11 (M.D. Fla. Aug. 7, 2013) (same) ("The Fourth Amendment does not require the level of surgical precision advocated by Defendant."). Following ***Cunnius*** would require this court to adopt the principle that constitutionally valid digital-data searches require imposition of controls not required for comparable searches of nondigital data. The State does not know of any authority — or reason — for this court to impose such a radical requirement.

Rindfleisch misperceives the import of ***Taylor***, 764 F. Supp. 2d 230. The court approved the use of a filter agent *after* the investigating officer unexpectedly encountered attorney-client correspondence while searching a collection of e-mail messages. ***Id.*** at 232. Moreover, the court in effect rejected the key propositions on which Rindfleisch predicates her challenge to the Gmail and Yahoo! warrants:

> 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. The Supreme Court has noted that, even "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." The First Circuit has said that "the police may look through . . . file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized." The same is true for the search of an e-mail account, and the search does not fail to satisfy the particularity requirement simply because the warrant does not specify a more precise e-mail search method.

Id. at 237 (footnotes omitted).

Rindfleisch fares no better with ***Mann***, 592 F.3d 779, and ***Bowen***, 689 F. Supp. 2d 675. In ***Mann***, the Seventh Circuit rejected the defendant's suggestion that the court adopt the procedures set out in ***United States v. Comprehensive Drug Testing, Inc.***, 579 F.3d 989 (9th Cir. 2009) (en banc) ("CDT II"), *revised and superseded by United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (en banc) ("CDT III"). Contrary to Rindfleisch's assertion that ***Mann*** "simply rejected a blanket prohibition of reliance on the plain view doctrine," Rindfleisch's Brief at 24, the Seventh Circuit essentially rejected Rindfleisch's view about digital-data protocols: "We are also skeptical of a rule requiring officers to always obtain pre-approval from a magistrate judge to use the electronic tools necessary to conduct searches tailored to uncovering evidence that is responsive to a properly circumscribed warrant." ***Mann***, 592 F.3d at 785.

As for ***Bowen***, 689 F. Supp. 2d 675, the district court recognized that the so-called "all records exception"

> "is not so much an 'exception' to the particularity requirement of the Fourth Amendment as a recognition that a warrant — no matter how broad — is, nonetheless, legitimate if its scope does not exceed the probable cause upon which it is based. The more extensive the probable wrongdoing, the greater the permissible breadth of the warrant."

Id. at 683 n.6 (citation omitted). Because the warrants in this case did not exceed the probable cause underlying them, the "all records exception" does not matter. Moreover, the prosecutor did not rely on the "all records exception" when he called the circuit court's attention to ***Bowen*** (36:3-4, R-Ap. 208-09). Rather, the prosecutor relied on ***Bowen*** for its main proposition: rejection of "Defendants' contention that the warrant lacked particularity because it failed to specify different or more precise computer search methods." ***Id.*** at 681.

B. Rindfleisch's As-Applied Challenge To The Constitutionality Of Wis. Stat. § 968.375 Goes Long On Rhetoric, Short On Analysis and Sense.

In barely more than two pages of her brief, Rindfleisch mounts a rhetorical attack on the application of Wis. Stat. § 968.375 here. She offers only two cases in support of her attack,[20] neither

---

[20] ***United States v. Liu***, 239 F.3d 138 (2d Cir. 2000); ***In re Termination of Parental Rights to Gwenevere T.***, 2011 WI 30, 333 Wis. 2d 273, 797 N.W.2d 854. Neither case cites Wis. Stat. § 968.375. A search of Westlaw's database of

(footnote continues on next page)

of which explains how or why the application of section 968.375 violated her constitutional rights.

Section 968.375 (reprinted at pp. 4-7, above) provides a mechanism for the Wisconsin attorney general or a Wisconsin district attorney to obtain, upon a showing of probable cause, "[t]he content of a wire or electronic communication" held "in electronic storage in an electronic communications system or held or maintained by a provider of remote computing service." Wis. Stat. § 968.375(4)(a). Rindfleisch fulminates:

> The state's sweeping application of section 968.375 in this case contradicts centuries of case precedent[21] intending to protect citizens of the United States and the State of Wisconsin from unreasonable searches and seizures. Neither Congress nor the Wisconsin Legislature is authorized to erase the constitutional rights of an investigation's target by use of warrants seeking to invade the target's privacy. Section 968.375, as applied here, erased Rindfleisch's rights.
>
> The broadly written statute not only changed existing law by giving Wisconsin circuit court judge's extraterritorial authority to issue warrants, but also provided a sweeping global opportunity to obtain electronic communications. The only way to ensure that the rights of users of electronic communications are not trampled by this law is to ensure that it is applied in a manner that recognizes the privacy protections afforded by the Constitution. Applying the statute in a manner that rides roughshod over pri-

---

(footnote continues from previous page)

Wisconsin cases did not turn up any case citing the statute, much less discussing it.

[21] In her two-page argument, Rindfleisch does not cite any case from the "centuries of case precedent" even hinting that the warrants in this case violated those precedents.

> vacy rights and allows the government to obtain personal private communications -- without particularizing the communications sought -- is unconstitutional and should not be condoned.

Rindfleisch's Brief at 32-33 (footnote added).

Rindfleisch's point remains obscure. She writes about "eras[ing] the constitutional rights of an investigation's target" (presumably meaning to classify her as the investigation's target at the time the John Doe court authorized the warrants). Rindfleisch's Brief at 33. 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. The State does not know of any Fourth Amendment doctrine that prohibits the State from seeking evidence from anyone who might have information about criminal conduct by a third person. Rindfleisch has not referred to any doctrine of that sort, either. Here, the warrants and supporting affidavit make clear that the State sought information from Rindfleisch about possible criminal conduct in which Tim Russell engaged. Consequently, the State's effort did not violate any Fourth Amendment doctrine or section 968.375.

In addition, the State does not know of any Fourth Amendment doctrine that prohibits a State from issuing a subpoena or warrant for service or execution in a different state. Rindfleisch has not referred to any doctrine of that sort, either. The Fourth Amendment requires only that a warrant issue "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the … things to be seized"; the

amendment does not include a territorial limitation. Whether an extraterritorial recipient of a subpoena or warrant complies with the demands might raise other issues, but none under the Fourth Amendment.

Rindfleisch asserts that "[s]ection 968.375, as applied here, erased [her] rights." Rindfleisch's Brief at 33. In her two pages of argument on this claim, she does not offer any actual explanation for her conclusory declaration. Presumably, she means that the Google and Yahoo! warrants fail to satisfy the requirements of the Fourth Amendment, an argument she makes elsewhere in her brief. But if the warrants violate the Fourth Amendment, whether the State followed the procedures in section 968.375 does not matter, making Rindfleisch's attack superfluous. On the other hand, if the warrants comply with the Fourth Amendment, Rindfleisch has not made any argument that the State failed to follow the procedures in section 968.375. And even if the State failed to follow the statutory procedure when obtaining Fourth Amendment-compliant warrants, the noncompliance would not amount to erasing her (or anyone's) constitutional rights.

In short, Rindfleisch's attack on the application of section 968.375 does not make any sense except as a renewal of the assault, in a different guise, on the warrants as not complying with the Fourth Amendment. Consequently, the challenge to the application of section 968.375 does not add anything benefiting Rindfleisch or harming the State.

C. Rindfleisch Makes a Meritless Argument About The Circuit Court's Reference To Rule 41(e)(2)(B) Of The Federal Rules Of Criminal Procedure.

In denying Rindfleisch's suppression motion, the circuit court referred to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure as buttressing the State's position regarding the constitutionality of a two-step procedure for obtaining and searching Rindfleisch's Gmail and Yahoo! e-mails (83:5, R-Ap. 446).[22] The two-step procedure in this instance consisted of, first, Google and Yahoo! each providing the State with a compact disc containing the e-mails from the specified account created by Rindfleisch (rellyk_us.yahoo.com and kmrindfleisch@gmail.com, respectively), and second, the State reviewing (*i.e.*, searching) the compact discs for e-mails relevant to the purpose for which the State sought them: as evidence of Tim Russell's misconduct in office.

---

[22] The federal rule provides persuasive authority, not mandatory authority, in support of the two-step seizure-and-search procedure used in this case. *See* ***United States v. Williams***, 650 F. Supp. 2d 633, 657 n.12 (W.D. Ky. 2009) ("Rule 41 of the Federal Rules of Criminal Procedure is not considered to be a rule of constitutional dimension that is applicable to the states." (citation omitted)). *Cf.* ***United States v. Schesso***, 730 F.3d 1040, 1051 (9th Cir. 2013) ("Because neither *CDT II* nor *CDT III* cast the search protocols in constitutional terms, state judicial officers cannot be faulted for not following protocols that were not binding on them, and law enforcement officers cannot be faulted for relying on a warrant that did not contain the non-binding protocols.").

Rindfleisch appears to believe that the two-step procedure for seizing and searching digital records violates the Fourth Amendment because "rationales [justifying removal of computers from a home or small business] … simply do not apply where the 'place to be searched' is a cyberspace 'cloud' of an internet service provider," and therefore that a search warrant for digital data should "[r]equir[e] an onsite search at a facility owned and operated by [an internet service provider like] Yahoo or GMail, which certainly would have the equipment necessary for the government to perform its review." Rindfleisch's Brief at 35. *See generally id.* at 34-36.

In support of her *ipse dixit*,[23] Rindfleisch cites . . . nothing. And for good reason. The Fourth Amendment does not say anything about whether a search of an evidence container — whether a physical box of paper documents or a digital "box" of digital documents — must occur at the original location of the container. The cases she called to the circuit court's attention, *see id.* at 35-36, demonstrate the point.

- In ***United States v. Winther***, 2011 WL 5837083 (E.D. Pa. Nov. 18, 2011), the warrant made clear that removal of the computer would occur for the convenience of the investigators. ***Id.*** at *3 ("The above seizure of computer and computer related hardware related to such computer related items as being the instrumentalities of crime and also to allow for analysis/search for evidence of crime in an appropriate forensic setting. *Up-*

[23] BLACK'S LAW DICTIONARY 905 (9th ed. 2009) ("[s]omething asserted but not proved").

on a determination that such examination would be more appropriately made in a controlled environment, the storage media may be removed and examined in a laboratory location." (emphasis added)). Moreover, in discussing Winther's contention that Rule 41(e)(2)(B)'s two-step procedure violated the Fourth Amendment, the court addressed Winther's contention that the two-step procedure resulted in a search outside the Rule 41(e)(2)(A)(i)'s fourteen-day period for executing a warrant, not the propriety of the two-step procedure itself. The court cited numerous cases holding that the two-step procedure, whether performed before or after Rule 41(e)(2)(B)'s amendment in 2009, did not violate the Fourth Amendment. ***Id.*** at *11-12.

- In ***United States v. Widner***, 2010 WL 4861513 (W.D.N.Y. Aug. 20, 2010) (magistrate judge's report and recommendation), *report and recommendation adopted in part and rejected in part*, 2010 WL 4861508 (W.D.N.Y. Nov. 30, 2010), the magistrate judge rejected Widner's contention "that the onsite preview provision is necessary to satisfy the warrant's particularity requirement." ***Id.*** at *6. Relying in part on advisory committee notes to Rule 41(e)(2)(B), the magistrate judge held "that the failure to conduct an onsite preview of the material seized did not render the warrant itself insufficiently particular or otherwise invalid." ***Id.*** at *7. In addition, the magistrate judge noted "that the agents would have discovered the child pornography whether the forensic preview had been conducted onsite, as

directed, or offsite, as in fact occurred." ***Id.*** at *8.

- In ***United States v. Kernell,*** 2010 WL 1491873 (E.D. Tenn. Mar. 31, 2010) (magistrate judge's report and recommendation), *report and recommendation adopted*, 2010 WL 1490921 (E.D. Tenn. Apr. 13, 2010), the magistrate judge, relying in part on advisory committee notes to Rule 41(e)(2)(B), held "that the forensic analysis of the data on the Defendant's computer without a written search methodology and in excess of the ten-day time limitation in Rule 41 does not violate the Fourth Amendment." ***Id.*** at *14. *See also* ***id.*** at *19 (citing ***Grubbs***, 547 U.S. at 98).
- In ***United States v. Roberts***, 2010 WL 234719 (E.D. Tenn. Jan. 14, 2010), the court, relying in part on advisory committee notes to Rule 41(e)(2)(B), held "that the forensic analysis of the data on the defendants' computers and on [the employer's] server without a written search methodology and in excess of the 10-day time limitation in Rule 41 does not violate the Fourth Amendment." ***Id.*** at *19. *See also* ***id.*** at *16 (citing ***Grubbs***, 547 U.S. at 98).

To put the point bluntly, the cases cited by Rindfleisch in support of her objection to the circuit court's reference to Rule 41(e)(2)(B) show, to the contrary, the pervasive balderdashery of her argument. The Fourth Amendment does not prohibit the two-step procedure permitted by the fed-

eral rule[24] and used here in accord with section 968.375. She has not identified any case holding the two-step procedure unconstitutional. She has not identified any case undermining the circuit court's reliance on Rule 41(e)(2)(B) as persuasive authority in support of the State's execution of its subpoenas and warrants.

In short, Rindfleisch appears to believe that under the Fourth Amendment, an investigator must travel to the site of an evidence container rather than have the container come to the investigator. The Fourth Amendment, however, does not impose any requirement of the sort, either for containers of digital evidence or for containers of nondigital evidence: whether the investigator goes to the container or the container comes to the investigator,[25] the container and its contents (and the container owner's interests) remain the same for purposes of applying Fourth Amendment search-and-seizure doctrines. The two-step procedure used in this case (and as set out in Rule 41) fully complies with the Fourth Amendment, and the authorities on which Rindfleisch relied show as much. Ultimately, Rindfleisch should feel relieved rather than aggrieved that the circuit court refrained from referring to the authorities she cited for support. *See* Rindfleisch's Brief at 36 (lamenting that "the circuit court never addressed those cases.").

---

[24] *See, e.g.,* ***United States v. Tylman***, 2007 WL 2669567, at *13 (C.D. Ill. Aug. 22, 2007); *see also* 36:7-8, R-Ap. 212-13.

[25] *Compare with* FRANCIS BACON, THE ESSAYS 64 (Scolar Press 1971) (1625) ("*If the Hill will not come to Mahomet, Mahomet wil go to the hil.*" (italicization in original)).

D. Because The Argument By Rindfleisch About The Warrants' Alleged Overbreadth Amounts To A Pared-Down Version Of Her Argument Alleging That The Warrants Lacked Sufficient Particularity, The State Relies On Its Earlier Argument On The Particularity Issue.

Rindfleisch offers a perfunctory (and heated) argument about the alleged overbreadth of the Google and Yahoo! warrants. *Id.* at 37-38. Her argument amounts to a truncated reiteration of her contention that the warrants lacked constitutionally sufficient particularity. *Compare id. with id.* at 17-20.

In response to Rindfleisch's overbreadth argument, the State relies on its earlier argument regarding the warrants' alleged lack of particularity (pp. 25-36, above).

E. Although This Court Should Hold That The Google And Yahoo! Warrants Complied With The Requirements Of The Fourth Amendment And Article I, Section 11 Of The Wisconsin Constitution, If This Court Concludes The Warrants Did Not Comply, The Court Should Remand The Case To The Circuit Court For An Evidentiary Hearing At Which The State Would Have An Opportunity To Show That The State Obtained Rindfleisch's Computer Laptop And Contents As A Result Not Of The Noncompliant Warrants, But Rather "'By Means Sufficiently Distinguishable To Be Purged Of The Primary Taint.'"

Rindfleisch objects that "the State provided no indicia that the seizure and search of Rindfleisch's personal laptop computer comported with the fourth amendment." Rindfleisch's Brief at 38 (capitalization modified). Her argument rests on her assumption that the Google and Yahoo! warrants violated the Fourth Amendment and that the seizure and search of her personal laptop computer violated the "fruit of the poisonous tree" doctrine. *Id.* at 39. *See, e.g.*, ***Wong Sun v. United States***, 371 U.S. 471, 488 (1963) (evidence obtained as a result of an illegal arrest becomes fruit of the poisonous tree that a court must exclude unless the government can show it obtained that evidence as a result not of the illegality, but rather "'by means sufficiently distinguishable to be purged of the primary taint'").

For reasons set forth previously in the State's brief, this court should conclude that the Google

and Yahoo! warrants comported with the Fourth Amendment and its counterpart in Article I, Section 11 of the Wisconsin Constitution.[26] If this court does so, this issue becomes moot. Even if the Google and Yahoo! e-mails provided the only basis for seizing and searching the laptop computer as a result of executing the search warrant in the Milwaukee County Executive's office,[27] the validity of the Google and Yahoo! warrants would preclude classifying the State's acquisition of the laptop and its contents as fruit of a poisonous tree.

On the other hand, if the court concludes that the Google and Yahoo! warrants violated the Fourth Amendment, the State agrees with Rindfleisch that the court should remand the case to the circuit court for a hearing at which the State would have an opportunity to "show that [the evidence] was obtained as a result not of the illegality, but rather 'by means sufficiently distinguishable to be purged of the primary taint.'"

F. For Fourth Amendment Purposes, Digital Data Does Not Differ From Nondigital Data In Sufficiently Significant Ways To Require Creating New Doctrines For Digital Data.

Rindfleisch contends that "continuing advances in technology mandate evolving considerations of the fourth amendment to protect citizens as a

---

[26] Wisconsin courts "ordinarily construe[ ] the protections of these provisions coextensively." ***State v. Artic***, 2010 WI 83, ¶ 28, 327 Wis. 2d 392, 786 N.W.2d 430.

[27] The State does not concede that the Google and Yahoo! e-mails provided the only basis for the warrant to search the Milwaukee County Executive's office.

matter of public policy." Rindfleisch's Brief at 40 (capitalization modified). *See generally id.* at 40-45. She cites only one case in support of her position: ***Cunnius***, 770 F. Supp. 2d 1138, a case twice rejected by the only court to have cited it.[28]

The State has already explained why this court should not allow the incantation "digital data" to operate as a distracting shiny object (pp. 18-24, above). Nonetheless, Rindfleisch hopes the court will find itself bedazzled by purported differences in kind rather than degree.

Although Rindfleisch offers an essay on a parade of potential horribles (none of which infect this case), her reliance on ***Cunnius*** misleads her. For example, she writes that "[w]hereas, a search warrant allowing search and seizure of a file cabinet is limited to the cabinet, search and seizure of a 'digital file cabinet' has no boundaries." Rindfleisch's Brief at 43. Not true. A "digital file cabinet" has limits, as her own case illustrates: "kmrindfleisch@gmail.com" defined the boundaries of the "digital file cabinet" subject to the Google warrant; seizure and search of that cabinet did not open a boundaryless seizure and search of other digital file cabinets in the gmail.com domain.

Elsewhere, she writes about using ISP personnel as filter agents:

> Whereas "a seize now, search later" approach may have [m]ade sense when the evidence to be seized was a filled file cabinet, this philosophy has no application where the files and file cabinet are digital

---

[28] See pages 43-44, above, for the State's response to Rindfleisch's initial reliance on ***Cunnius***.

> records maintained by an ISP. Digital records containing specific email addresses or user names can be easily sorted by ISP personnel, who then can search those records for specific names or other language without opening and reading private, confidential emails that are unrelated to the alleged criminal offenses giving rise to the warrants.

Id. at 44. Here, of course, ISP personnel selected records containing specific e-mail addresses — "kmrindfleisch@gmail.com" and "rellyk_us@yahoo .com" — thus satisfying her first criterion. But even assuming an ISP would agree to allowing employees to become *de facto* criminal investigators[29] (and Rindfleisch offers no argument or evidence that any ISP would agree to assume this obligation), she naively assumes that searching by keywords rather than viewing a digital document would suffice for capturing all data within the scope of a warrant or for excluding "private, confidential emails that are unrelated to the alleged criminal offenses giving rise to the warrants."

For instance, keyword searches would prove useless for evaluating nontext files (such as scanned-PDF files not made text-searchable via processing by a PDF-compatible optical-character-recognition function). Moreover, keyword searching comes with an array of drawbacks that would deprive investigators of evidence within the scope of a valid warrant.[30]

---

[29] Highly unlikely. *See generally* Brief of Amici Curiae Yahoo!, Inc. et al. in Support of Appellant, *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), 2002 WL 32107853.

[30] *See* Ralph Losey, *Sedona's New Commentary on Search, and the Myth of the Pharaoh's Curse*, e-Discovery Team (Sept. 16, 2007, 8:23 p.m.), **Error! Hyperlink refer-**

(footnote continues on next page)

In effect, by urging this court to impose protocols that would not make a whit's worth of difference in her case, Rindfleisch asks this court to issue an advisory opinion. This court should reject her invitation. This court need not acquiesce in her "shiny object" distraction.

(footnote continues from previous page)

ence not valid. (last visited Apr. 10, 2014); *see also* CHRISTOPHER G. WREN & JILL ROBINSON WREN, USING COMPUTERS IN LEGAL RESEARCH: A GUIDE TO LEXIS AND WESTLAW 15-21 (1994) (orientation to database searching); *id.* at 23-67 (search terms and logic connectors); *id.* at 148-64 (formulating search requests, and discussing semantic problems); *id.* at 769-70 (discussing recall/precision trade-off).

CONCLUSION

For the reasons offered in this brief, this court should affirm the circuit court's order denying Rindfleisch's suppression motion challenging the Google and Yahoo! warrants and should affirm the judgment of conviction.

Date: April 11, 2014.

Respectfully submitted,

J.B. VAN HOLLEN
Attorney General

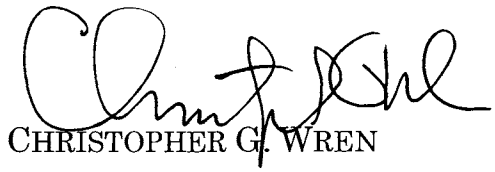
CHRISTOPHER G. WREN
Assistant Attorney General
State Bar No. 1013313

Attorneys For Plaintiff-
Respondent State of Wisconsin

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 266-7081
wrencg@doj.state.wi.us

CERTIFICATE OF COMPLIANCE WITH WIS. STAT. § (RULE) 809.19(8): FORM AND LENGTH REQUIREMENTS

In accord with Wis. Stat. § (Rule) 809.19(8)(d), I certify that this brief satisfies the form and length requirements for a brief and appendix prepared using a 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, maximum of 60 characters per line, and a length of 10,352 words.



CHRISTOPHER G. WREN

CERTIFICATE OF COMPLIANCE WITH WIS. STAT. § (RULE) 809.19(12): ELECTRONIC BRIEF

In accord with Wis. Stat. § (Rule) 809.19(12)(f), I certify that I have submitted an electronic copy of this brief (excluding the appendix, if any) via the Wisconsin Appellate Courts' eFiling System and that the electronic copy complies with the requirements of Wis. Stat. § (Rule) 809.19(12).

I further certify that the text of the electronic copy of this brief is identical to the text of the paper copy of the brief.

A copy of this certificate has been served with the paper copies of this brief filed with the court and served on all opposing parties.

CHRISTOPHER G. WREN

CERTIFICATE OF COMPLIANCE WITH WIS. STAT. § (RULE) 809.19(2)(A):

SUPPLEMENTAL APPENDIX

In accord with Wis. Stat. § (Rule) 809.19(3)(b), I certify that filed with this brief, either as a separate document or as a part of this brief, is a supplemental appendix that complies with the confidentiality provisions of Wis. Stat. § (Rule) 809.19(2)(a). I certify that if the record is required by law to be confidential, the portions of the record included in the appendix are reproduced using first names and last initials instead of full names of persons, specifically including juveniles and parents of juveniles, with a notation that the portions of the record have been so reproduced to preserve confidentiality and with appropriate references to the record.

CHRISTOPHER G. WREN