RECEIVED
06-13-2013
CLERK OF COURT OF APPEALS
OF WISCONSIN

STATE OF WISCONSIN
COURT OF APPEALS
DISTRICT I

STATE OF WISCONSIN,

Plaintiff-Respondent,

Appeal No. 2013AP000362
Milw. Cty. Case No. 12-CF-438

vs.

KELLY M. RINDFLEISCH,

Defendant-Appellant.

DEFENDANT-APPELLANT KELLY M. RINDFLEISCH'S BRIEF AND APPENDIX

APPEAL FROM THE ORDER DENYING MOTION TO SUPPRESS ENTERED ON SEPTEMBER 14, 2012 AND THE JUDGMENT AND CONVICTION ENTERED ON NOVEMBER 27, 2012, IN THE CIRCUIT COURT OF MILWAUKEE COUNTY, HONORABLE DAVID A. HANSHER PRESIDING,

---

FRANKLYN M. GIMBEL
State Bar. No. 1008413
Email: fgimbel@grgblaw.com
KATHRYN A. KEPPEL
State Bar No. 1005149
Email: kkeppel@grgblaw.com
Attorneys for Defendant-Appellant
Kelly M. Rindfleisch

GIMBEL, REILLY, GUERIN & BROWN LLP
Two Plaza East, Suite 1170
330 East Kilbourn Avenue
Milwaukee, Wisconsin 53202
Telephone: 414/271-1440

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

PAGE

PAGE

PAGE

Statutes and Other Sources

INTRODUCTION

This case involves the circuit court's interpretation and application of state and federal law governing search warrants issued to out-of-state entities Yahoo and Google (Gmail) by a Wisconsin circuit court judge presiding over a John Doe proceeding. Defendant Kelly M. Rindfleisch moved to suppress the fruits of those search warrants on grounds that the sweeping nature of the warrants, purportedly permitted by the Wisconsin Legislature's enactment of section 968.375, *Stats.*, eviscerated her privacy rights under the Fourth and Fourteenth amendments of the United States Constitution and correlative provisions of the Wisconsin Constitution, as well as potentially running afoul of other constitutional protections, including her rights under the First and Sixth Amendments and HIPPA laws.

In essence, the state's response to Rindfleisch's suppression motion was that it is entitled to conduct a fishing expedition via overly broad warrants without

any screening system to preclude prosecutors from reviewing privileged or otherwise sensitive information. Ignoring the grave invasion of privacy that results when the state is granted such overreaching authority, the circuit court adopted the state's position, thereby rendering the Fourth Amendment meaningless with respect to search of digital and electronic data.

STATEMENT OF THE ISSUE

Did the circuit court err when it denied Rindfleisch's motion seeking suppression of emails obtained by the state via warrants issued to Yahoo and GMail?

Not answered by circuit court.

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

Oral argument is appropriate in this case because it would provide the Court and counsel an opportunity to explore the interplay between the language of the Wisconsin and federal statutes, the cases interpreting the statute and other applicable federal precedent. Argument also would provide an opportunity to

address current societal concerns regarding limits – or lack thereof – on the government's ability to access information about and from private citizens through the use of technology.

Publication of this Court's decision is appropriate because no reported Wisconsin decision specifically addresses these issues. This case will establish precedent for the admission of digital evidence obtained from internet service providers located outside the State of Wisconsin.

STATEMENT OF THE CASE

A. Nature of the Case.

This case arises from allegations that Rindfleisch engaged in partisan campaign activities on Milwaukee County time. (R.3). These allegations are based in part on email communications Rindfleisch allegedly had related to campaign activities and, specifically for purposes of this appeal, email communications that were seized by investigators through a broad exercise of warrants issued by the Milwaukee County Circuit

Court to internet service providers outside the State of Wisconsin. (*Id.*).

B. Course of Proceedings.

On January 26, 2012, the state filed a criminal complaint against Rindfleisch charging her with four counts of misconduct in public office, a felony, contrary to section 946.12(3), *Stats*. (*Id.*). Based on the complaint and according to discovery provided to defense counsel, prior to initiating charges, the state sought and obtained general investigative search warrants to collect information and evidence from out-of-state ISPs Yahoo and Gmail relative to Rindfleisch's personal email accounts with those entities. (R.26:1-8;App.115-120).

The search warrant directed to Yahoo provides:

> (a) The contents of all communications stored in the Yahoo accounts for the subscriber(s) identified above, including all emails stored in the account, whether sent from or received in the account as well as e-mails held in a "Deleted" status;
>
> (b) All records or other information regarding the identification of the accounts, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the

IP address used to register the accounts, log-in IP addresses associated with session times and dates, account statuses, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

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

(R.26:1-4;App.115-17). The search warrant directed to Gmail provides:

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

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

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

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

(R.26:5-8;App.118-20).

Rindfleisch moved to suppress the evidence obtained via the search warrants on grounds that the warrants lacked the required level of particularity and were overly broad. (R.23-R.26). On August 21, 2012, the court issued an order from the bench denying the motion. (R.83:9-10;App.112-13). A written order denying the motion was entered on September 14, 2012. (R.51;App.103). Rindfleisch petitioned this Court for leave to appeal the circuit court's decision, but that petition was denied on October 2, 2012. (R.66).

Following extensive plea negotiations, on October 11, 2012, Rindfleisch entered and the court accepted a plea of guilty to one count of misconduct in public office, a Class I felony, in violation of section 946.12(3), *Stats*. (R.84:14-20). Rindfleisch appeared for sentencing on November 19, 2012. (*See*

R.78;App.101). The circuit court withheld sentence and placed Rindfleisch on probation for a period of three years, imposed a six month period of confinement with Huber release privileges in the House of Correction, and ordered her to pay costs and surcharges. (R.78;App.101-02).

Judgment of conviction was entered on November 27, 2012 (R.78;App.101-02), and Rindfleisch filed a timely notice of intent to pursue post-conviction relief on the same date. (R.79). Rindfleisch filed a timely notice of appeal on February 12, 2013. (R.80).

C. Disposition Below.

Rindfleisch was convicted of one count of felony misconduct in public office. She was ordered to serve a probation term of three years, plus six months confinement, with release privileges, in the House Correction as a condition of her probation. (R.78;App.101-02).

STATEMENT OF FACTS

The facts relevant to this appeal are generally undisputed. Rindfleisch was hired as a policy advisor for Governor Scott Walker while he was still Milwaukee County Executive in early 2010. (R.3:3). She was promoted to Deputy Chief of Staff in March 2010. (R.3:4). As a Milwaukee County employee, Rindfleisch was issued a laptop computer and an email account: Kelly.Rindfleisch@milwcnty.com. (*See* R.24:3). In addition, Rindfleisch had a personal laptop computer and cell phone for which she created and owned personal email accounts with internet service providers (ISPs) Yahoo and Gmail: rellyk_us@yahoo.com and kmrindfleisch@gmail.com, respectively. (*See* R.26:2,6;App.115,118).

In late 2010, as part of a John Doe investigation into activities of colleagues of Governor Scott Walker while he was still Milwaukee County Executive, law enforcement officials delved into communications among Walker's County Executive staff, the staff for his

gubernatorial campaign and the campaign staff for lieutenant governor candidate Brett Davis. (R.3:2-3). As part of their investigation, law enforcement officials requested and obtained warrants issued to unknown employees at Yahoo and Gmail to obtain "all communications" stored in the Yahoo and Gmail accounts for the email addresses identified above, including all emails stored in the account, whether received at or sent from the account. (R.26:2,6;App.115,118). The ISPs produced the information pursuant to the warrants, and it was disclosed as part of the criminal complaint. (*See* R.3; *passim*).

As noted above, Rindfleisch moved to suppress all evidence obtained via the search warrants issued to Yahoo and Gmail on grounds that doing so violated her constitutional rights. (R.22-R.26). In denying her motion, the circuit court determined that search warrants requiring an unknown employee of an ISP to produce "all" of a person's email records was not

constitutionally defective as overbroad read as a whole, that the warrants authorized the search of specific email accounts for a specific period for specific crimes, and, even if the warrants were overbroad, they should not be suppressed because the search was not in "flagrant disregard for the limitations" of the warrant. (R.83:8;App.111).

STANDARD OF REVIEW

This Court reviews the denial of a motion to suppress evidence under a two-part standard of review. The Court upholds the circuit court's findings of fact unless they are clearly erroneous; however, the Court reviews *de novo* whether those facts warrant suppression. *State v. Hampton,* 2010 WI App 169, ¶23, 330 Wis. 2d 531, 543-44, 793 N.W.2d 901.

The interpretation and constitutionality of a statute "as applied" are questions of law reviewed *de novo. In re Gwenevere T.*, 2011 WI 30, ¶19, 333 Wis. 2d 273, 284-85, 797 N.W.2d 854.

ARGUMENT

THE CIRCUIT COURT ERRED WHEN IT DENIED RINDFLEISCH'S MOTION TO SUPPRESS THE INFORMATION OBTAINED FROM HER YAHOO AND GMAIL ACCOUNTS.

Rindfleisch acknowledges she did not have a reasonable expectation of privacy in her employer-provided computer and her Milwaukee County email account. She did, however, have a reasonable expectation of privacy and cognizable rights to privacy and protection from intrusion relative to her own personal computer, mobile phone, and personal emails, text messages and mobile phone communications. This expectation of privacy is recognized and protected by the Fourth and Fourteenth Amendments and correlative provisions of the Wisconsin Constitution, as well as various federal and state statutes. *See City of Ontario v. Quon*, 560 U.S. ___, 130 S.Ct. 2619, 2630 (2010). Email communications are entitled to the same strong Fourth Amendment protections traditionally afforded to telephone and letter communications. *United States v. Warshak*, 631 F.3d 266, 285-87 (6th Cir. 2010). An email

subscriber enjoys a reasonable expectation of privacy in the contents of her private emails that are stored with, sent or received through a commercial internet service provider. *Id.* at 288. So, too, for cell phone subscribers' text messages. *See State v. Clampitt*, 364 S.W.3d 605, 611 (Mo. Ct. App. 2012) (citing *Warshak)*.

Absent a valid warrant, any search of records maintained by ISPs constitutes a violation of the Fourth Amendment. *Warshak,* 631 F.3d at 288; *Clampitt,* 364 S.W.3d at 611. Thus, if the warrants issued to Yahoo and GMail were deemed to be general warrants -- and if the state failed to make an adequate showing of probable cause as to why ***all*** of Rindfleisch's emails and texts had to be searched as part of the state's investigation -- the search of Rindfleisch's computer, Yahoo and Gmail account information, emails, text messages and cell phone communications violated her constitutional rights. Therefore, all evidence obtained via those warrants and the fruit of the evidence should

have been suppressed and the circuit court's order denying the motion must be reversed.

A. Search Warrants Are Required To Identify The Objects To Be Seized With Requisite Particularity.

The United States Supreme Court "has consistently asserted that the rights of privacy and personal security protected by the Fourth Amendment " . . . are to be regarded as of the very essence of constitutional liberty; and that the guaranty of them is as important and as imperative as are the guaranties of the other fundamental rights of the individual citizen." *Harris v. United States*, 331 U.S. 145, 150 (1947). The Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings. *See Marron v. United States,* 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant

describing another. As to what is to be taken, nothing is to be left to the discretion of the officer executing the warrant.").

Thus, the Fourth Amendment prohibits the issuance of any warrant that does not describe the objects to be seized with particularity. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). General warrants do not satisfy the Fourth Amendment requirement that the warrant contain a description of the place to be searched and the person or things to be seized. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976); *United States v. Jones*, 54 F.3d 1285, 1290 (7th Cir. 1995). The particularity requirement guards against the government indiscriminately rummaging through a person's property for evidence about any and every possible crime under the sun. *Jones*, 54 F.3d at 1290.

A warrant must be specific enough that the officers involved in its execution are able to identify the things to be seized with reasonable certainty. *United States v. Spears*, 965 F.2d 262, 277 (7th Cir. 1992).

"[W]arrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized." *United States v. Leary*, 846 F.2d 592, 600 (10th Cir. 1988) (internal citations omitted). The "[f]ailure to employ the specificity available will invalidate a general description in a warrant." *United States v. Cook*, 657 F.2d 730, 733 (5th Cir. 1981). In addition to preventing general searches, a sufficiently particularized warrant also assures that the individual whose property is searched or seized is aware of the lawful authority of the executing officer, his need to search and the scope and limits of his power to search. *Groh v. Ramirez*, 540 U.S. 551, 561 (2004).

Law enforcement officers must be especially careful when seeking authority to seize a broad class of information such as documents or computer data. *See, e.g., Leary*, 846 F.2d at 603 n.18 ("search warrants for documents are generally deserving of somewhat closer scrutiny with respect to the particularity requirement

because of the potential they carry for a very serious intrusion into personal privacy") (internal citations omitted). So, too, is closer scrutiny required for search warrants issued to obtain emails, texts and other forms of electronic communication.

The basic standard of particularity remains as the United States Supreme Court stated it nearly eighty years ago. "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. at 196; *see also Jones*, 54 F.3d at 1290. "The Fourth Amendment bans exploratory rummaging (which diminishes privacy) and excessive seizures (which interfere with property)." *United States v. Bentley*, 825 F.2d 1104, 1110 (7th Cir. 1987).

B. The Warrants Issued To Yahoo And GMail Lack The Level Of Particularity Required To Pass Constitutional Muster.

The warrant applications and affidavits in this case, and the warrants themselves, fail to establish probable cause that all of the information the state sought constituted evidence of any crime or evidence, and if so, what. *See United States v. Stubbs*, 873 F.2d 210 (9th Cir. 1989) (warrant describing generic categories of documents without any effort to specifically describe the items which the officers could have seized under a probable cause standard); *Leary*, 846 F.2d at 602-03 ("'By listing every type of record that could conceivably be found in an office, the warrant effectively authorized the inspectors to cart away anything they found on the premises'") (quoting *Roberts v. United States*, 656 F.Supp. 929, 934 (S.D.N.Y. 1987)). Here, the warrants required unknown employees of the ISPs to produce all of their records, and then left it to law enforcement officers to sift through Rindfleisch's personal, private

communications to determine which of those communications actually related to their case.

What happened here is exactly what long-established law prohibits. 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. Such general warrants permitting exploratory rummaging and excessive searches, violate the Fourth and Fourteenth Amendments and their Wisconsin constitutional correlatives.

Unknown employees of the ISPs complied with the warrants, allowing law enforcement to review all of Rindfleisch's emails, which could have included matters clearly privileged under the law, such as communications with her attorneys or physicians, protected under the Sixth Amendment and HIPPA,

respectively, as well as correlative Wisconsin law. The emails could have contained Rindfleisch's communications with her pastor or spiritual provider. They could have included personal communications with family members or even intimate communications with a loved one. Under the warrants, the ISPs were required to produce a myriad of categories of communications, none of which had any relationship or relevance to the state's investigation. The absence of any limitations or particularity as to the items to be produced rendered the warrants constitutionally defective.

The warrants also lacked sufficient particularity because, as courts have recognized, there are methods available to law enforcement officers to enable them to identify particular computer files and minimize the intrusion of protected privacy rights without searching files outside the scope of a warrant. For example, in searching a computer, "observing file types and titles listed on the directory, doing a keyword search for

relevant terms, or reading portions of each file stored in the memory" were suggested as means to search for specific records without rummaging through all records in *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999). As the *Carey* court noted:

> Computer programs store information in a wide variety of formats. For example, most financial spreadsheets store information in a completely different format than do word processing programs. Similarly, an investigator reasonably familiar with computers should be able to distinguish database programs, electronic mail files, telephone lists and stored visual or audio files from each other. Where a search warrant seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records.

Id. at 1275, n.8 (quoting Winick, "Searches and Seizures of Computers and Computer Data," 8 HARV. L.J. & TECH. 75, 108 (1994)).

C. The Circuit Court Misapplied *Bowen*, *Taylor* and *Mann*.

In its ruling below, the circuit court held that pre-screening or other limitations have been held not to be *required* in the Fourth Amendment context. (R.83:3;App.106). Apparently, the circuit court

interpreted that language to allow law enforcement officers carte blanche to subpoena and seize a citizen's computer records and digital information, provided they later rifle through these personal documents to find evidence to justify their search. In reaching this conclusion, the court ignored caselaw supporting Rindfleisch's position and instead adopted caselaw that is factually distinguishable.

In *United States v. Cioffi,* 668 F.Supp.2d 385 (E.D.N.Y.2009), the court granted a suppression motion "when faced with a similar warrant authorizing the search of all emails in a defendant's email account." The *Cioffi* court determined that "because the search warrant affidavit did not limit the search to emails related to the alleged crime and did not incorporate by reference the affidavit containing the description of the alleged crime and the associated use of the target email account, the warrant lacked particularity." *Cioffi,* 668 F.Supp.2d at 392. "[A]uthorization to search for 'evidence of a crime,' that is to say, any crime, is so

broad as to constitute a general warrant . . . [*A*]*fortiori* a warrant not limited in scope to any crime at all is . . . unconstitutionally broad." *Id.* (quoting *United States v. George,* 975 F.2d 72, 77 (2d Cir. 1992)).

Although the circuit court found that *Cioffi* contained "interesting and insightful" thoughts about computer searches under the Fourth Amendment, and the "unique concerns" posed by such searches, the court gave *Cioffi* no weight because it found the case was not "on point" and was a district court case and not a federal circuit case. (App.106-07). Nonetheless, the court had no problem adopting the holdings in two other federal district courts.

One of those cases was *United States v. Bowen*, 689 F.Supp.2d 675 (S.D.N.Y. 2010), where the court relied on the "all records" exception applicable where the investigation target is an enterprise that "is primarily engaged in unlawful activity and sufficient evidence is presented on the pervasiveness of that unlawful activity with the enterprise." *Bowen*, at 683. Unless the state is

prepared to argue that the office of the Milwaukee County executive was "primarily engaged in unlawful activity," *Bowen* and its "all records" exception cannot be applied here.

The other case was *United States v. Taylor*, 764 F.Supp.2d 230, 237 (D. Me. 2011), which actually favors Rindfleisch. The *Taylor* court denied the defendant's suppression motion because the prosecution used a "filter agent" to review the records before the prosecuting authorities saw them. A zip drive was provided by Microsoft and a government agent began reviewing the header information of the emails (sender, recipient, date and subject) and realized the zip drive contained emails to or from the defendant's lawyers. The agent then stopped his review and contacted the prosecutor, after which the government filed a motion with the court proposing that a "filter agent" not associated with the prosecution review the emails and cull out any potentially privileged materials before either the investigating agent or prosecutor received

them. The court entered the order, the filter agent reviewed the emails, privileged materials were provided to defense counsel and the balance of the materials was provided to the prosecutor and investigating agent. *Id.* at 232.

In denying the suppression motion, the *Taylor* court concluded that the government acted reasonably by using a filter agent and the defense failed to present an alternate proposal for reviewing the records. *Id.* at 234-35. Here, no filter agent was utilized and Rindfleisch was not ever given the opportunity to present an alternate proposal. Rather than support the circuit court's ruling, *Taylor* provides protections the circuit court apparently deemed unnecessary in Rindfleisch's case.

The circuit court also relied on *United States v. Mann*, 592 F.2d 779 (7th Cir. 2010). However, the circuit court misunderstood that ruling. The *Mann* court simply rejected a blanket prohibition of reliance on the plain view doctrine, stating that it preferred to "allow

the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication." *Id.* (quoted source omitted). The circuit court acknowledged that *Mann* was decided before *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (*en banc*) ("*CDT III*"), a case arising from the government's investigation of use of steroids and performance-enhancing drugs in professional sports. The *CDT III* court determined that the following safeguards were necessary to protect citizens: "(1) that investigative agents not review and segregate the data; (2) that specialized forensic computer search personnel review and segregate the data and not give it to the investigative agents; and (3) seized evidence outside the scope of the warrant be returned within 60 days."

The court reasoned that "[b]road searches of ESI devices create 'a serious risk that every warrant for electronic information will become, in effect, a general

warrant, rendering the Fourth Amendment irrelevant.'" *Id.* at 1176. Indeed, the *CDT III* court recognized

> . . . the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.

Id. at 1176–77).

The circuit court's conclusion that the Seventh Circuit would reject this holding based on *Mann* was purely speculative. Rindfleisch urges this Court to give full consideration to the *CDT III* court's reasoned analysis of the need to protect our citizens from blanket, general search warrants allowing government invasion of privacy.

D. The Circuit Court Ignored The *Cunnius* Decision.

In her papers supporting her suppression motion, Rindfleisch cited *In re U.S.'s Application For A Search*

Warrant To Seize & Search Elec. Devices From Edward Cunnius, 770 F.Supp.2d 1138 (W.D. Wash. 2011). *Cunnius* discussed the need for courts to reevaluate the application of dated Fourth Amendment law when considering searches and seizures involving technology. In doing so, the court noted the significant difference between searching file cabinets and searching digital records:

> A search of a file cabinet, in contrast, would include only items put in the file cabinet by a person. A conscious, even if unknowing, act is required. This act perhaps would be analogous to intentionally downloading a file. However, in contrast to the conscious act of downloading a file or storing something in a file cabinet, cache files are a set of files automatically stored on a user's hard drive by a web browser to speed up future visits to the same websites, without the affirmative action of downloading. *See U.S. v. Romm,* 455 F.3d 990, 993 n.1 (9th Cir. 2006). *See also U.S. v. Parish,* 308 F.3d 1025, 1030–31 (9th Cir. 2002). "Most web browsers keep copies of all the web pages that you view up to a certain limit, so that the images can be redisplayed quickly when you go back to them." *Romm*. Thus, a person's entire online viewing history can be retrieved from the cache, without any affirmative act other than visiting a web page.

Id. at 1145-46. The court then identified another factor distinguishing a limitless digital search to a file cabinet search: information and data can be removed from a

file cabinet and destroyed; digital data cannot. *Id*. at 1146.

The *Cunnius* court began its analysis by citing a history lesson of decisions holding that general search warrants violate the Fourth Amendment:

- "The Fourth Amendment's particularity provision was enacted to respond to the evils of general warrants and writs of assistance which English judges had employed against the colonists." *Virginia v. Moore,* 553 U.S. 164, 169 (2008).

- The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book;" since they placed "the liberty of every man in the hands of every petty officer." *Boyd v. United States,* 116 U.S. 616, 625 (1886) (internal footnotes omitted).

- The requirement was thus designed to ensure only a specific place is searched and that probable cause to search that place actually exists. *See Steele v. United States,* 267 U.S. 498, 501–02 (1925).

770 F. Supp.2d at 1142-43. The court then stated:

> Contrary to the Fourth Amendment's particularity requirement limiting searches to only the specific areas and things for which there is probable cause to search, the government seeks to scour everything contained in the digital devices and information outside of the digital devices. This practice is akin to the revenue officers in colonial days who scoured "suspected places" pursuant to a general warrant.

Id. at 1143.

The court then discussed aspects of a digital search, including the vast quantities of information captured and the fact that such searches capture innocent and personal information with no relevance to the asserted offenses. *Id*. at 1144. In addition to concerns about unknowingly downloaded data and destroyed data set forth above, the court expressed specific concerns about the fact that the digital devices provided a "portal" through which the government

could obtain other data, especially given that the government requested passwords, password files and encryption codes, noting that such codes allow the government "to access a defendant's most sensitive information" and noted that the devices could contain information such as medical records, emails sent or received by the defendant's wife (who was not accused of any criminal activity), books the couple were reading, movies they were watching and even legal "dirty pictures." *Id*. at 1145.

Finally, the *Cunnius* court addressed *CDT III*, noting *CDT III*'s endorsement of the warrant issuing magistrate's action in imposing procedural safeguards to ensure that the search would comport with the Fourth Amendment. *Cunnius,* at 1149. The court rejected the government's argument in C*unnius* that procedural safeguards were neither necessary nor required, despite the breadth of the warrant requested. The court also rejected the notion that the "plain view" doctrine allowed the government to seize and retain

information obtained outside the scope of the warrant. *Id* at 1151.

In the end, the *Cunnius* court rejected the warrant application, finding that because the government refused to perform the search with constitutional safeguards such as a filter agent and foreswearing reliance on the plain view doctrine, the warrant did not pass constitutional muster.

In Rindfleisch's case, the court issuing the warrants did not impose any safeguards to ensure that the warrants were not overbroad or otherwise failed to pass constitutional muster. The State provided no evidence indicating that it took any action to ensure that investigators and prosecutors did not review privileged materials or materials unrelated to the charged offenses. Despite this, the circuit court ignored *Cunnius* and its thorough and balanced analysis of the need for safeguards to ensure that warrants comported with the Fourth Amendment. Instead, the court approved overly broad searches that trampled Rindfleisch's

rights, and set the precedent for continued trampling of rights in future cases.

E. Section 968.375 Is Unconstitutional As Applied In This Case.

Although statutes are presumed constitutional, the law does ***not*** presume that the statute "was applied in a constitionally sufficient manner." *In re Gwenevere T.*, at ¶¶47-49, 333 Wis. 2d at 299-300. Rather, the court must analyze the constitutional right adversely affected by application of the statute. *Id.* at ¶49, 333 Wis. 2d at 300.

In enacting section 968.375, *Stats.*, the Legislature, apparently recognizing the changes in communications brought about by the electronic age, attempted to create a means for law enforcement officers to access that data to seek evidence of criminal activity. The state's sweeping application of section 968.375 in this case contradicts centuries of case precedent 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 privacy rights and allows the government to obtain personal private communications -- without particularizing the communications sought -- is unconstitutional and should not be condoned.

In situations like this, suppression of all evidence seized is appropriate because the government effected a

widespread seizure of items that were not within the scope of the warrant. *See United States v. Lin*, 239 F.3d 138, 140 (2d Cir. 2000). When the application of a law collides with one's constitutional rights, the law must give ground.

F. The Seizure And Copying Provision Of Rule 41(e)(2)(B) Does Not Trump The Fourth Amendment.

The circuit court also justified upholding the search warrants on grounds they were sanctioned by Rule 41(e)(2)(B), as amended in 2009. (*See* R.83:5;App.108). Rindfleisch concedes that the 2009 comment to the rule provides for a "two-step process." That the state employed a two-step process to obtain the data, however, does not mean the state's execution of that two-step process comported with the Fourth Amendment as discussed above.

The state relied below on *United States v. Tylman*, 2007 WL 2669567 (C.D. Ill. 2007) (not reported) as a case where the two-step process was employed prior to the amendment. The issue in *Tylman* was simply whether

the agents were authorized to remove computers from the defendant's residence or whether they were required to search the computers there. The court noted it would be impractical to conduct the search at the residence and that doing so would be much more intrusive to the homeowners. Those rationales may apply when investigators are physically taking up space in someone's home or small business, but they simply do not apply where the "place to be searched" is a cyberspace "cloud" of an internet service provider. Requiring an onsite search at a facility owned and operated by Yahoo or GMail, which certainly would have the equipment necessary for the government to perform its review, would not create the burdens justifying removal in *Tylman*.

Rindfleisch presented to the circuit court four cases addressing Rule 41(e)(2)(B) since its amendment in late 2009. None of those cases involved warrants served on internet service providers; all involved searches at the defendant's residence or place of

employment: *United States v. Winther*, 2011 WL 5837083 (E.D. Pa. Nov. 18, 2011) (warrant for search of defendant's residence and seizure of computer); *United States v. Widner,* 2010 WL 4861513 (W.D.N.Y. Aug. 20, 2010) (same); *United States v. Kernell,* 2010 WL 1491873, (E.D. Tenn. Mar. 31, 2010) (same); *United States v. Roberts,* 2010 WL 234719, at 19–20 (E.D.Tenn. Jan. 14, 2010) (warrant for search of defendant's place of employment and computers). As in *Tylman*, the rationales for removing the computers in these cases do not apply when the place to be searched is cyberspace or, at best, the headquarters of an internet company such as Yahoo or GMail. Yet, the circuit court never addressed those cases.

Finally, nothing in Rule 41(e)(2)(B) suggests that utilizing the two-step process sanctifies a warrant and execution thereof from a Fourth Amendment challenge. To the extent the circuit court believed it does, the court committed constitutional error and its decision must be reversed.

G. The Warrants Were Overbroad.

The circuit court determined that the warrants were not overbroad -- even though they required Yahoo and GMail to produce "all communications" – because law enforcement officers were only authorized to search for specific crimes. This conclusion defies common sense.

The general rule is that items seized within the scope of a search warrant need not be suppressed simply because other items were seized that were outside the scope of the warrant. *State v. Petrone,* 161 Wis. 2d 530, 548, 468 N.W.2d 676 (1991). This is true ***unless*** the search was conducted in "flagrant disregard for the limitations of the warrant." *Id.*

The circuit court found no flagrant disregard for the limitations of the warrant. How could there be? The warrant had no limitations. The warrant required production of ***all*** communications, which could have included privileged and non-privileged and irrelevant

communications with family members, friends, health care providers, financial planners and even clergy.

The warrant allowed state investigators to search ***all*** communications in order to find the evidence of campaign activity during specified time periods. This allowed investigators to rifle through personal, privileged communications without limitations. The court's conclusion that the warrants were not overbroad under these circumstances ignored Rindfleisch's constitutional and civil rights and should be reversed.

H. The State Provided No Indicia That The Seizure And Search Of Rindfleisch's Personal Laptop Computer Comported With The Fourth Amendment.

Illegally obtained evidence must be suppressed under the *same* evidence was obtained from an independent source. *Murray v. United States,* 487 U.S. 533, 537-38 (1988). In *State v. Nawrocki,* 2008 WI App 23, ¶38, 308 Wis. 2d 227, 253, 746 N.W.2d 509, the court remanded for an evidentiary hearing on the issue of whether an in-court identification was based on an

independent source unlimited by an impermissible showup identification. The same rationale applies here – an evidentiary hearing was required at which the state was obliged to prove that it had an independent source untainted by the illegal search warrants for its evidence against Rindfleisch.

Yet, despite these requests, the circuit court found without a hearing that the emails were independently obtained through seizure of Rindfleisch's personal laptop. In accepting the state's argument without requiring the state to present any evidence, the circuit court ignored the critical question. Where did the state obtain the passwords and codes necessary to access information from Rindfleisch's laptop? If this information was the fruit of the warrants issued to Yahoo and GMail, it is fruit of the poisonous tree and should have been suppressed.

Rindfleisch requested an evidentiary hearing at which the state would be required to establish that the information was in fact obtained independently,

producing evidence establishing how its investigators acquired the information necessary to access Rindfleisch's computer. The circuit court's denial of that request violated Rindfleisch's constitutional rights. Therefore, her conviction should be reversed and this case remanded for an evidentiary hearing

I. Continuing Advances In Technology Mandate Evolving Considerations Of The Fourth Amendment To Protect Citizens As A Matter Of Public Policy.

Within recent weeks American citizens have learned that the government has been monitoring their mobile devices, their social media posts, tweets and blogs, and generally has used technology to invade the privacy of citizens for no reason other than "to protect national security." While this goal is laudable, ignoring the civil liberties of American citizens is not.

Technology provides a wealth of means for investigators to invade privacy without leaving any clues that they snuck into our "cyber-houses" without prior notice. It allows investigators to learn not only

whether we are posting manifestos about overtaking the government, but also to see what we "like" on Facebook, whom we "follow" on Twitter, whether we read the *Wall Street Journal* or *People* online, and what other websites we accessed on the worldwide web.

In most cases, this spying is harmless, who cares that we read about or comment on a starlet's new haircut or a financial planner's recommendation. But what happens when the pages we access and comments we make are personal and constitutionally or statutorily privileged? Should the government be allowed to know a citizen searched WebM.com for alternate cancer treatments? What about a search for help beating a heroin addiction? Is it not arguable that a search related to how to stop using illegal drugs could be "fair game" because the searcher must be committing the criminal offense of possessing the drug?

These concerns regarding government review of personal use of technology are exacerbated when the government authorizes a search warrant for ***all***

communications stored in a citizen's email account. As discussed above, such language allows an investigator to read private communications between a citizen and his or her lawyer, priest, rabbi, physician, psychiatrist or spouse. It allows access to private medical information intended to be shared only with family and close friends. Absent limits, every bit of personal information ever placed in cyber-space is fair game, despite the Bill of Rights.

This is the environment in which we live, and federal and state laws interpreting the Fourth Amendment and its state corrollaries have yet to catch up. As the *Cunnius* court explained in its thoughtful and well-reasoned analysis, digital searches are different. They capture vast quantities of data, including innocent and personal information with no relevance to the asserted crimes. *Cunnius,* 770 F.Supp.2d at 1144.

Moreover, because digital data acts as a portal to other devices and data, a warrant authorizing seizure of

"all" communications is limitless. *Id.* at 1145. Whereas, 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. Whereas file cabinets contained only the information placed in the drawers, computer hard drives automatically store files without the user's knowledge. Similarly, while information can be removed from a file cabinet, digital information is extremely difficult to remove or destroy. *Id.* at 1145-46.

As the *Cunnius* court stated:

> … a balance must be struck between the government's investigatory interests and the rights of individuals to be free from unreasonable searches and seizures. Few computers are dedicated to a single purpose …. Almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation.

Id. at 1151-52 (quoted source omitted). Cognizant of that need to strike a balance, the *Cunnius* court mandated constitutional safeguards. The circuit court's ostrich-like view in not even commenting on the need for constitutional safeguards in this case ignores the

evolving nature of federal investigation and the application of the Fourth Amendment to authorizing the search for and seizure of digital information.

The question presented here is whether decades-old Fourth Amendment jurisprudence remains viable in assessing warrants issued for digital information. Whereas "a seize now, search later" approach may have 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 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. Antiquated rationales for seizing first and reviewing later must give way to considerations of newer, more efficient means of searching created by technological advances.

As those advances continue and more offices go "paperless," courts will continue to face challenges to the seizure and search of digital records. The orderly administration of justice requires courts to analyze carefully the Fourth Amendment's application to such records. Rindfleisch urges this Court to address these issues, and to reach the same conclusion as the *Cunnius* court. In balancing the government's need to investigate with the constitutional rights of citizens, warrants authorizing search and seizure of digital information must include constitutional safeguards to protect civil rights.

CONCLUSION

The state's warrant affidavit/application failed to set forth with the required level of particularity the items to be provided under the warrant, resulting in the production of ***all*** emails sent and received via Rindfleisch's personal email accounts. Although section 968.375 provides the state an opportunity to obtain such electronic communications, enactment of

that statute should not be applied in a manner allowing for law enforcement officers to ignore their requirement to particularize items subject to the search and to allow them to rummage through personal electronic communications in a fishing expedition to find an email to support their investigation.

The state's fishing expedition in this case violated Rindfleisch's rights under the Fourth and Fourteenth Amendments, correlative provisions under the Wisconsin Constitution, and, perhaps, her rights under the First and Sixth Amendments, her right to engage in privileged communications with certain professionals and her general constitutional right to privacy.

Finally, continuing advances in technology require this Court and all state and federal courts reconsider past interpretations of the Fourth Amendment and strike new balance between the needs of government and the rights of its citizens.

For all of these reasons, defendant-appellant Kelly M. Rindfleisch respectfully urges this Court to

reverse the circuit court's denial of her suppression motion, vacate her conviction and remand this case for further proceedings.

Dated this _____ day of June, 2013.

GIMBEL, REILLY, GUERIN & BROWN LLP

By:

_____

FRANKLYN M. GIMBEL
State Bar. No. 1008413
Email: fgimbel@grgblaw.com
KATHRYN A. KEPPEL
State Bar No. 1005149
Email: kkeppel@grgblaw.com
Attorneys for Kelly M. Rindfleish

POST OFFICE ADDRESS:

Two Plaza East, Suite 1170
330 East Kilbourn Avenue
Milwaukee, Wisconsin 53202
Telephone: 414/271-1440

CERTIFICATION PURSUANT TO SECTION 809.19(8)(d), *STATS*.

Pursuant to section 809.19(8)(d), *Stats.*, I certify that this brief conforms to the rules contained in section 809.19(8)(b) and (c) for a document produced with a proportional serif font. The length of this brief is 7,319 words.

_____

KATHRYN A. KEPPEL

CERTIFICATION PURSUANT TO SECTION 809.19(2)(b), *STATS*.

I hereby certify that filed with this brief, either as a separate document or as a part of this brief, is an appendix that complies with section 809.19(2)(a) and that contains, at a minimum:

(1) a table of contents;
(2) the findings or opinion of the circuit court; and
(3) portions of the record essential to an understanding of the issues raised, including oral or written rulings or decisions showing the circuit court's reasoning regarding those issues.

I further certify that if this appeal is taken from a circuit court order or judgment entered in a judicial review of an administrative decision, the appendix contains the findings of fact and conclusions of law, if any, and final decision of the administrative agency.

I further 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.

_____
KATHRYN A. KEPPEL

CERTIFICATION PURSUANT TO SECTION 809.19(12)(f), *STATS*.

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

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

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.

_____
KATHRYN A. KEPPEL

CERTIFICATION PURSUANT TO SECTION 809.19(13), *STATS*.

I hereby certify that I have submitted an electronic copy of this appendix, which complies with the requirements of section 809.19(13), *Stats.*

I further certify that this electronic appendix is identical in content to the printed form of the appendix filed as of this date.

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

_____
KATHRYN A. KEPPEL