RECEIVED
05-20-2014
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 REPLY BRIEF

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

Statutes and Other Sources

INTRODUCTION

The Fourth Amendment reflects the determination of those who wrote the Bill of Rights that United States should "'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant." *Stanford v. Texas*, 379 U.S. 476, 509–10, (1965) (quoting U.S. Const. amend. IV)). The state's seizure of "***all***" of Kelly M. Rindfleisch's private emails and related records eviscerated any sense of security from government intrusion. The state seized from her internet service providers "***all***" records related to her email addresses, including the content of her emails, under the guise of seeking evidence of criminal conduct by a third party.

Rindfleisch challenged the searches and seizures as violative of her Fourth Amendment rights and her constitutional right to privacy. The circuit court and the state have flatly rejected Rindlfeisch's position. Indeed, in its response brief, the state cavalierly, and at times

belittlingly, characterizes Rindfleisch's arguments supporting her assertion of her constitutional rights as "rhetoric," "nonsense" and "baldashery," while claiming its warrants -- requiring production of "***all***" records related to her email addresses, without limitation – passed constitutional muster.

Until the United States Supreme Court rules on this issue, state and federal courts will have varying opinions on what levels of protections courts should impose. One court favors use of a filter agent. *In re U.S.'s Application For A Search Warrant To Seize & Search Elec. Devices From Edward Cunnius*, 770 F.Supp. 2d 1138, 1144 (W.D. Wash. 2011), a protocol Rindfleisch urges this Court to adopt. Other courts, equally troubled by broad general warrants seeking all emails and all other content related to email accounts, focus on the particularity requirement and overbreadth of warrants, rejecting them for lack of probable cause and/or a linkage/nexus between the records and the crimes alleged. *See Matter of Search of Info. Associated with*

[Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc. (Apple), 2014 WL 1377793 (D.D.C. Apr. 7, 2014); *In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts,* 2013 WL 4647554 (D.Kan. Aug. 27, 2013).

Rindfleisch urges this Court to find the state's warrants lacked the particularity and the linkage/nexus necessary to ensure the warrants did not tread on her constitutional rights to privacy and freedom from unreasonable searches and seizures.

REPLY ARGUMENT

I. The Wide-Ranging Searches Available To Law Enforcement Through Search Warrants For Digital Data Require Greater Scrutiny Of A Warrant's Particularization Of The Items To Be Seized.

Rindfleisch is neither dazzled by digital data nor transfixed by any bright shiny object. She simply asserts a truth recognized by courts and legal scholars -- digital data ***is*** different.

"With the rise of the internet, the government has an increasing need to examine e-mails and files stored

by ISPs. At the same time, the digital age ***heightens the privacy concerns implicated by broad searches and seizures of stored e-mail -- as compared to the days of paper records***." Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971, 986-87 (2012) (citing *United States v. Comprehensive Drug Testing, Inc. (CDT III)*, 621 F.3d 1162, 1177 (9th Cir. 2010)) (emphasis added). An email account likely contains not only emails possibly relevant to an investigation, but also emails and files "the government has no probable cause to search and seize." *Id.* (citing *CDT III*, at 1176; *United States v. Cioffi*, 668 F. Supp. 2d 385, 391 (E.D.N.Y. 2009)). Greater vigilance by judicial officers is required to strike "the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures." *Id.* (citing *CDT III*, at 1177). Officers must ensure searches and seizures of stored emails occur in a manner minimizing

unwarranted intrusions upon privacy. *Id*. (citing *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1967)).

As explained in *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999), because electronic storage likely contains a greater quantity and variety of information than previous storage methods, "computers make tempting targets in searches for incriminating information." (Quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data,* HARVARD J.L. & TECH. 75, 104 (1994). Email accounts are not equivalent to file drawers, boxes or other "data containers." "Relying on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'" *Id.*

Digital searches not only capture vast quantities of data, including innocent and personal information with no relevance to the asserted crimes, but also provide a limitless portal to other devices, data and

individuals, rendering a warrant authorizing seizure of "***all***" communications limitless. *Cunnius*, 770 F.Supp. 2d 1138 at 1144-45. The ability to store and intermingle a huge array of personal information and papers in one place "increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and ***accordingly makes the particularity requirement that much more important***." *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (emphasis added).

II. The Circuit Court Erred When It Denied Rindfleisch's Suppression Motion.

A. The Search Warrants Issued In This Case Were General Warrants Authorizing The State *Carte Blanche* To Scour Rindfleisch's Private Emails.

The warrant clause of the Fourth Amendment serves two constitutional protections. First, it eliminates all searches not based on probable cause: any intrusion via search or seizure is an evil, so no intrusion is justified "without a careful prior determination of

necessity." *Coolidge v. New Hampshire,* 403 U.S. 443, 467 (1971). Second, "searches deemed necessary should be as limited as possible." *Id*. "The "specific evil" to be protected against is the general warrant, thus, the problem is not the intrusion *per se*, but "a general, exploratory rummaging in a person's belongings." *Id*. Requiring a "particular description" of the things to be seized accomplishes the limitation objective. *Id*. The particularity requirement also provides assurances to individuals whose property is searched or seized that the executing officer has lawful authority, the need to search, and the power to search limited by the warrant. *Groh v. Ramirez*, 540 U.S. 551, 561 (2004).

A search warrant lacks the required particularity when it, as the warrants did here, authorizes the search of "***all***" emails in a citizen's email account without linking all of the requested records to criminal activity. *See Cioffi,* 668 F.Supp.2d at 392; *see also Cunnius, Target,* and *Apple,* all *supra.*

The state contends its warrants are sufficient, providing the contents of the warrants in a table. The table refers to "¶¶(a)-(d)" and "¶¶(a)-(c)" under the category "Records to Produce." Those paragraphs do ***not*** particularly describe the items to be seized, nor do they contain any link or nexus to any alleged crime. Instead, they broadly demand from Yahoo: "the contents of ***all*** communications stored" in its account (including emails); "***[a]ll*** records or other information regarding the identification of the accounts" and "***[a]ll*** records pertaining to communications between Yahoo, Inc. and any person regarding the accounts[.]" (R.26:1-4;App.115-17). From Gmail (Google) they demanded the same records as requested from Yahoo plus "***[a]ll*** address books … or any other similar compilations of personal contact information associated with the accounts." (R.26:5-8;App.118-20).

The state failed to provide probable cause for, yet and its warrants permitted the seizure of, "***all***" communications associated with the nominated

Rindfleisch email accounts during a specified period of time, without any other limitation whatsoever. These general warrants authorizing the state to rummage through Rindfleisch's private communications violated Rindfleisch's constitutional right to freedom from such searches and seizures and to privacy.

B. The Cases Rindfleisch Cited Support Her Position.

As is common in appellate advocacy, Rindfleisch cited some cases for the general principles of law, not because their ultimate rulings supported her position. For example, she cited *United States v. Stubbs*, 873 F.3d 210 (9th Cir. 1989), for the general proposition that a warrant generically describing documents to be seized is insufficient, and *United States v. Leary,* 846 F.2d 592 (10th Cir. 1988), for language criticizing warrants identifying every conceivable record found in an office to justify taking everything.

Rather than "flatly misrepresent[ing]" the *Carey* decision, Rindfleisch accurately quoted *Carey's* adoption of the Winick law review article quoted above.

Moreover, *Carey* rebuffed the government's proffered "file cabinet" analogy because the search involved electronic data, declaring that when law enforcement encounters intermingled relevant and irrelevant documents, the officer must stop pending a magistrate's approval of "the conditions and limitations on a further search." *Carey*, 172 F.3d at 1275.

The state argues the only two cases citing *Cunnius* rejected its reasoning supporting a filter agent. Notably, both cases were authored by the same judge, who adopted the recommendations of the same magistrate judge. Thus, a single court disagrees. Moreover, the state's summary dismissal of *Cunnius*, without any discussion of its well-reasoned analysis of issues in this case, suggests the state was unable to attack the analysis and instead sought a side door to avoid it.

The state argues *United States v. Taylor*, 764 F.Supp.2d 230, 237 (D. Me. 2011), where the court denied the defendant's suppression motion because the

prosecution used a "filter agent" to review the records before the prosecuting authorities saw them, was inapplicable because that court ordered the filter agent only after confidential materials were discovered. Rindfleisch cited *Taylor* only to establish using a filter agent was appropriate to cull potentially privileged materials and did not violate the Fourth Amendment. *See id.* at 234-35.

Rindfleisch agrees *United States v. Bowen*, 689 F.Supp.2d 675 (S.D.N.Y. 2010), has no application here. *Bowen* relied on the "all records" exception applicable where the investigation target is an enterprise primarily engaged in pervasive unlawful activity. *Bowen*, at 683. Thus, *Bowen* distinguished itself from *Cioffi*, a case supporting Rindfleisch's position, where the court suppressed a warrant authorizing the search of all emails in a defendant's email account for lack of particularity. *Id.*; *Cioffi,* 668 F.Supp.2d at 392.

The state's suggestion Rindfleisch misapplied *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010), is

simply wrong. *Mann* rejected a call to completely abandon the plain view doctrine. *Id.* at 785. While "skeptical" of a rule requiring pre-approval where a warrant is "properly circumscribed[,]" the court counselled those searching digital data to exercise caution to ensure warrants describe with particularity the things to be seized and searches are narrowly tailored "to uncover only those things described." *Id*. at 786.

Here, the warrant-issuing court failed to ensure they passed constitutional muster. The circuit court, ignoring soundly-reasoned analyses of other courts, rejected the need for some safeguards -- whether they be filter agents or greater scrutiny to ensure compliance with the particularity requirement -- and erroneously affirmed the state's use of overly-broad general warrants and searches, trampling Rindfleisch's constitutional rights.

C. Section 968.375 Is Unconstitutional As Applied.

The state characterized Rindfleisch's section 968.375 argument as "fulminating," "rhetoric" and "superfluous" and also criticized her for citing only two cases and not identifying the "centuries of precedent" supporting her position. Rindfleisch is not sure if the state is merely attempting to misdirect the Court or is being deliberately obtuse.

Rindfleisch's argument builds upon the preceding arguments of her brief, including her prior citation of the Fourth Amendment (ratified in 1792, *see State v. Tye*, 2001 WI 124, 248 Wis. 2d 530, 536, 636 N.W.2d 473), and 20th and 21st Century caselaw interpreting the Fourth Amendment. She was not railing, raging or ranting. Nor was her argument mere rhetoric or obscure. Building on her prior arguments, Rindfleisch challenged the statute as applied to her.

Search warrants issued under section 968.12, *Stats.*, are limited to searches and executions of warrants within Wisconsin. Section 968.375, *Stats.*, contains no

geographical limitation. Thus, when enacted, section 968.375 granted Wisconsin courts new, sweeping extraterritorial authority to issue warrants to obtain electronic communications.

Moreover, the statute places no limits on items subject to a search warrant, authorizing warrants seeking "[t]he content of a wire or electronic communication" in storage and other records and information defined by statute. Sec. 968.375(3), *Stats*. Depending on how it is applied, this provision has the potential to trample the constitutional rights of Wisconsin citizens by authorizing broad general warrants for "***all***" records related to a particular email account. That is exactly what happened here. The court's authorization of the state's request for a warrant to obtain all of Rindfleisch's records, without scrutinizing the warrants to ensure they particularized the items to be seized, violated her constitutional rights.

D. Compliance With Rule 41(e)(2)(B) Does Not Establish A Warrant Passes Constitutional Muster.

Rindfleisch does not contend Rule 41(e)(2)(B)'s two-step process itself violates the Fourth Amendment. Her initial brief cited the cases the state cites at pages 41-43 only to establish the Rule's two-step process had not been the subject of any judicial scrutiny in the context of warrants authorizing seizure of emails and other electronically stored data, as opposed to computer hardware.

Rindfleisch maintains the judicial rationales for the two-step process -- the impracticality of searching a computer at a target's residence, the intrusive effect of doing so, etc. -- simply do not apply where the "place to be searched" is a cyberspace "cloud" of an internet service provider. Although the state criticizes Rindfleisch for citing no authority supporting this position, the state cites no authority to the contrary.

Since Rindfleisch filed her initial brief, Magistrate Judge David Waxse has determined the process does

violate the Fourth Amendment. In *Target Email Accounts/Skype Accounts*, 2013 WL 4647554 at *8, he held warrants authorizing an ISP to disclose "all" email communications, including content, and all records and other information regarding the account were "too broad and too general" because they failed to set any limits on the information to be provided to the government. The warrants required the ISP to disclose, without restrictions, all email communications in their entirety and all information about the account. The court was most troubled by the warrants' failure to limit the universe of electronic communications and information to be produced to the specific crimes being investigated. *Id*. The court added that even if it were to allow such broad warrants, they "would still not pass Constitutional muster" because they failed to set any limits on the government's review of the information and did not identify any sorting or filtering procedures for information that was irrelevant, outside the scope of

the government's probable cause statement, or attorney-client privileged information. *Id*.

More recently, Magistrate Judge John Facciola reluctantly agreed he was bound by precedent upholding the two-step process, but held that courts still must "incorporate appropriate minimization procedures into the warrants to comply with the Fourth Amendment." *In Matter of Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, 2013 WL 7856600 *6 (D.D.C. Nov. 26, 2013). He questioned the underlying premise of Rule 41 -- law enforcement had to open every file and folder to search effectively -- based on the "sea change" in how computers containing enormous amounts of data are searched with new technology. *Id*.

Just last month, Judge Facciola again addressed Rule 41(e)(2)(B), holding government warrants were invalid despite complying with the Rule's two-step process. *Apple*, 2014 WL 1377793 at *5. The Rule is

constitutional "under certain circumstances" in that it creates a "***narrow exception***" -- "but only if the government provides an adequate search protocol explaining how it will perform the search and ensure that it is only searching sectors or blocks of the drives that are most likely to contain the data for which there is probable cause." *Id*. (Emphasis added). He stated the government continued to abuse the Rule 41 process by submitting warrants requiring complete disclosure of the entire contents of an email account. *Id*. He concluded the best alternative, which is both in accordance with the Fourth Amendment, and prevents seizure of large quantities of data without probable cause, would be for the ISP to perform the search and produce any relevant data it discovers. *Id*. at *6.

These authorities demonstrate compliance with Rule 41(e)(2)(B) does not itself guarantee compliance with the Fourth Amendment and an individual's right to privacy. The circuit court's conclusion it did was constitutional error and should be reversed.

E. Digital Data Requires Different Considerations.

This brief cites several cases and authorities supporting Rindfleisch's position that search warrants seeking digital data must be scrutinized differently from paper or other tangible items under the Fourth Amendment. *Cunnius, Cioffi, Target, Facebook, and Apple* may have different ideas of how to accomplish this task, but they agree the limitless reach provided by the portal of an email address requires something more – whether it be a filter agent, an ISP employee review or simply requiring more detailed particularization of the items to be seized. As the Ninth Circuit stated:

> … when it comes to the seizure of electronic records, [overseizing] 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.

CDT III, 621 F.3d at 1177.

Perhaps privacy rights and the Fourth Amendment do not make a "whit's worth of difference" to the state, but Rindfleisch holds her constitutional protections dear. Wisconsin must adopt a procedure balancing the state's interest in law enforcement and the right of individuals like Rindfleisch to be free from unreasonable searches and seizures.

CONCLUSION

Defendant-appellant Kelly M. Rindfleisch respectfully urges this Court to reverse the circuit court's ruling denying the suppression motion, vacate her conviction and remand this case for further proceedings.

Dated this _____ day of May, 2014.

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 2,984 words.

_____
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