IN THE SUPREME COURT
STATE OF WISCONSIN

STATE OF WISCONSIN,

Plaintiff-Respondent-Respondent,

vs. **Appeal No. 2013AP000362-CR**

KELLY M. RINDFLEISCH,

Defendant-Appellant-Petitioner.

PETITION FOR REVIEW AND APPENDIX OF KELLY M. RINDFLEISCH

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

PAGE

TABLE OF AUTHORITIES

Cases

PAGE

PAGE

Statutes and Other Sources

INTRODUCTION

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

State v. Rindfleisch, Dkt. #2013AP362(D) at ¶¶43 and 46 (November 12, 2014) (Fine, J. dissenting). These three sentences written by the late Court of Appeals Judge Ralph Adam Fine succinctly express why the majority's decision must be reviewed by this Court.

This case involves the circuit court's interpretation and application of state and federal law governing search warrants issued to two out-of-state internet service providers by a Wisconsin circuit court judge presiding over a John Doe proceeding. Defendant-appellant-petitioner Kelly M. Rindfleisch moved to suppress the fruits of those search warrants on grounds that the sweeping nature of the warrants

rendered them general warrants, eviscerating her rights under the Fourth and Fourteenth Amendments to 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 HIPAA laws.

There can be no dispute that Rindfleisch had a reasonable expectation of privacy and cognizable rights to privacy and protection from intrusion relative to her 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 the contents of 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 internet service providers 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 Rindfleisch's internet service providers are tantamount to 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 purportedly authorized by those warrants violated her constitutional rights.

Ignoring the grave invasion of privacy that results when the state is granted such overreaching authority, the Court of Appeals affirmed the circuit court's adoption of the state's position, thereby rendering the Fourth Amendment meaningless in Wisconsin with respect to searches for digital and electronic data. Rindfleisch urges this Court to accept review to address the constitutionality of such virtually unfettered searches of the digital and electronic data of Wisconsin's citizens.

STATEMENT OF THE ISSUES

1. Where no probable cause exists to believe an individual has committed any offense, is a search warrant authorizing the unfettered collection of ***all*** of that individual's emails from her internet service provider for a specified period of time, without use of a screening agent or some other process to ensure confidentiality of private matters unrelated to the purpose of the warrant, unreasonable, overbroad and violative of the constitutional rights of the individual?

The majority of the Court of Appeals found no constitutional violation, holding that the warrants issued in this case met the requirements of the Warrants Clause and that no information exceeding the scope of the warrants was produced.

2. In light of the proliferation of personal and private emails and other electronic and digital data stored on the servers of internet service providers, over which the individual "owner" of the data has no control, should Wisconsin adopt a protocol requiring that a filter agent or other protections be utilized in executing a search warrant for an individual's emails and other electronic or digital data to ensure that individual's constitutional right to privacy?

The Court of Appeals found no reason to distinguish electronic and digital data from papers contained within a file cabinet, noting that officers often would have to separate documents for which seizure was authorized from other documents. The Court of Appeals concluded that no filter agent or similar

protocol was necessary to ensure the constitutionality of a search for electronic and digital data.

STATEMENT OF CRITERIA FOR REVIEW

Rindfleisch asks this Court to accept review of the Court of Appeals' decision affirming the circuit court's denial of her motion to suppress search warrants authorizing law enforcement officers unlimited and unscreened access to her personal email accounts.

The primary need for review is that this case involves real and significant questions of both federal and state constitutional law: an individual's rights under the Fourth and Fourteenth Amendments, and correlative provisions of the Wisconsin Constitution, to be free from unreasonable searches and seizures of private, personal digital and electronic information and communications, as well as the constitutional right to privacy with respect to such communications. *See* sec. 809.62(1r)(a), *Stats*. In recent years, many courts around the country, mostly federal courts, have

considered this issue, resulting in a variety of differing opinions and protocols[1].

The United States Supreme Court has not squarely addressed constitutional issues related to seizure of email communications; however, its recent opinion in *Riley v. California*, ___ U.S. ___, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014), holding that law enforcement officers may not search cell phones incident to a warrantless arrest without first obtaining a warrant, recognizes that electronic and digital information is quantitatively and qualitatively different from physical records, *id.* at 2490, a distinction the

[1] *See*, *e.g.*, *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010); *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010); *In Matter of Search of Info. Associated with [Redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc. (Apple)*, 13 F.Supp.2d 157 (D.D.C. August 8, 2014), vacating 2014 WL 1377793 (D.D.C. Apr. 7, 2014); *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 (D.D.C. Nov. 26, 2013); *In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts,* 2013 WL 4647554 (D.Kan. Aug. 27, 2013); *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); *United States v. Taylor*, 764 F.Supp.2d 230 (D. Me. 2011); *United States v. Bowen*, 689 F.Supp.2d 675 (S.D.N.Y. 2010); *United States v. Cioffi*, 668 F. Supp. 2d 385 (E.D.N.Y. 2009).

Court of Appeals rejected in this case. *Rindfleisch*, at ¶40. (App.121).

This Court should accept review not only to address this conflict between the Court of Appeals' decision and *Riley*, sec. 809.62(1r)(d), *Stats.*, but also to establish Wisconsin law governing the constitutional limits of law enforcement officers' ability to access and use as evidence an individual's personal, private email communications. Sec. 809.62(1r)(b), *Stats.*

An opinion by this Court also will develop Wisconsin law governing the constitutionality of search warrants and searches seeking to recover the personal emails of an individual and the admissibility of such evidence. As no reported Wisconsin decision specifically addresses this issue, an opinion will establish precedent for the admission of electronic and digital communications obtained from internet service providers. Sec. 809.62(1r)(c)1, *Stats.*

Review by this Court also is necessary because the opinion of the Court of Appeals majority allows the

state to continue to conduct fishing expeditions of individuals' digital data via overly broad warrants without any screening system to preclude prosecutors from reviewing privileged or otherwise sensitive information entitled to constitutional privacy protections. Given the increasing use of electronic communication via email and social media, such issues are certain to recur unless this Court takes action. Sec. 809.62(1r)(c)3, *Stats*.

STATEMENT OF THE CASE

Rindfleisch seeks review of the Court of Appeals' decision issued on November 12, 2014, rejecting her appellate challenge to the circuit court's denial of her motion to suppress evidence, namely private email communications to and from Rindfleisch, obtained via search warrants from her internet service providers.

It is undisputed that neither the search warrants nor the affidavits supporting those warrants implicated Rindfleisch in any improper behavior. *Rindfleisch*, at ¶¶44-45 (App.124, 126). Instead, the state was seeking

evidence against another of Governor (then Milwaukee County Executive) Walker's associates, Tim Russell. *Id*., at ¶¶5-6, 30. (App.104-05, 116-17). The affidavits of the state's investigator asserted that evidence of ***Russell's*** misconduct would be found in Rindfleisch's email accounts. *Id*. at ¶6. (App.104). According to the state, Rindfleisch's alleged culpability became "apparent" only after prosecutors received the warrant return. *Id*. at ¶45. (App.126).

Even though the state acknowledged it lacked any belief that Rindfleisch was involved in any improper activity when the warrants were issued, the state relied on the seized email communications in charging her. (See R.1). The state filed a criminal complaint charging Rindfleisch with four counts of felony misconduct in public office, contrary to section 946.12(3), *Stats*. (R.3). Rindfleisch moved to suppress the evidence obtained via the search warrants on grounds that the search and seizure violated her constitutional rights, arguing *inter alia* that the warrants

lacked the required level of particularity and were overly broad. (R.23-R.26). The circuit court denied the motion. (R.83:9-10;App.139-40;R.51;App.130). A petition for leave to appeal the circuit court's decision was denied. (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). 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 and ordered her to pay costs and surcharges. (R.78;App.128-29). Rindfleisch filed a timely notice of appeal. (R.80). Her conviction was affirmed by a 2 to 1 majority of the District I Court of Appeals on November 12, 2014. (App.101-27).

The facts relevant to this appeal are generally undisputed and set forth in the Court of Appeals'

decision. *Rindfleisch*, at ¶¶2-16. (App.102-10). As part of their investigation of Tim Russell, law enforcement officials requested and obtained warrants issued to unknown employees at Yahoo and Google to obtain "all communications" related to Rindfleisch's email accounts with those entities. Specifically, the search warrant directed Yahoo to provide:

> (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.

The search warrant directed Google to provide the same materials, plus:

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

Rindfleisch, at ¶¶7-8. (R.26:1-4;App.105-06, **115-17**).

Rindfleisch argued that all evidence obtained via the search warrants issued to Yahoo and Google should be suppressed on grounds the warrants violated her constitutional rights. (R.22-R.26). In denying her motion, the circuit court determined these search warrants, requiring an unknown employee of an ISP to produce "all" of a person's email records, were not constitutionally defective as overbroad read as a whole, that they 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.138).

A majority of the Court of Appeals affirmed the circuit court's ruling, with Judge Ralph Adam Fine dissenting. *Rindfleisch, supra.* (App.101-27).

ARGUMENT

I. This Court Should Review The Court Of Appeals' Application Of The Protections Of The Fourth Amendment To Searches For Electronic And Digital Data.

A. Searches Of The Private, Personal Email Communications Of Individuals Who are Not Suspected Of Any Criminal Behavior Are Unreasonable And Violate The Fourth Amendment.

The Court of Appeals majority focused on whether the search warrants issued to Yahoo and Google met the requirements of the Warrants Clause: authorization by a neutral and detached magistrate; a demonstration of probable cause that evidence will be found in a particular location; and a particularized description of the place to be searched. *Rindfleisch*, at

¶23 (citing *State v. Sveum*, 2010 WI 92, ¶20, 328 Wis. 2d 369, 787 N.W.2d 317). (App.123).

In his dissent, Judge Fine strongly disagreed with the majority's conclusion that the state's failure to demonstrate probable cause that Rindfleisch was involved in criminal wrongdoing had no bearing on its analysis, finding that allowing law enforcement officers *carte blanche* to rummage through Rindfleisch's digital files to find evidence of ***her*** **i**mproper conduct under the guise and authority of searching for evidence of ***Russell's*** crime violated her rights and was "illegal." *Rindfleisch*, at ¶44. (App.123-24). Neither the warrants nor the supporting applications and affidavits in this case set out probable cause that Rindfleisch had committed a crime or described any place where evidence that she had done anything wrong could be found. *Id.* (App.124). As Judge Fine explained, the particularity requirement "'makes general searches . . . impossible' because "it prevents the seizure of one thing under a warrant describing another.'" *Id.* (quoting

United States v. Ganias, 755 F.3d 125, 134-35 (2d Cir. 2014).

The majority criticized Judge Fine's analysis, stating that two cases on which it relied, *United States v. Adjani*, 452 F.3d 1140 (9th Cir. 2006) and *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), hold that a third party's culpability is irrelevant. *Rindfleisch*, at ¶¶29-30. (App.116). Those decisions, however, are neither on point nor unchallenged.

Adjani involved a warrant to search the computer hard drive of Reinhold, the cohabitating partner of their suspect, Adjani. The computer was the same computer from which officers observed Adjani sending emails. In essence, Reinhold's privacy interest in her computer and its contents was compromised by allowing Adjani to use it. *Adjani* is easily distinguishable on its facts. Rindfleisch and Russell were not romantically involved, did not live together, did not share a computer and, most important, there was no basis for the courts below to conclude that she shared any of her personal, private

email communications with Russell. Moreover, the holding in *Adjani* has been put into question by the Ninth Circuit's *en banc* ruling in *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010), which is discussed below.

Zurcher is also distinguishable. In that case the third party was a newspaper office, which published photographs of a demonstration at which officers were assaulted. *Zurcher*, 436 U.S. at 551. A warrant authorized law enforcement officers to search for photographs, negatives, films and other records, records that obviously would be found at the office given the publication of the photographs the day before. Since *Zurcher* was decided, Congress has enacted the Privacy Protection Act (PPA) protecting newspapers and similar entities from such searches. *See* 42 U.S.C. §2000aa *et seq.*

It is antithetical to Fourth Amendment jurisprudence to allow law enforcement officers to search all of an individual's private, personal electronic

and digital files without limitation, without notice and without cause. At the time most Fourth Amendment jurisprudence was decided, individuals could protect their personal letters, photographs or other documents by simply destroying them, resting easy knowing that those documents never would see the light of day. With electronic and digital data, however, nothing is ever truly destroyed. Technical experts can obtain documents from computer servers and even documents never transferred to anyone can be recovered from computer hard drives.

Under the Court of Appeals' decision, ***any*** document, once emailed to another person, is fair game for review by law enforcement officers, no matter that law enforcement has no probable cause, not even a reasonable suspicion that the individual whose records are being searched has committed a crime. This rationale is no different from the mindset of Colonial revenue officers that led to the creation of the Fourth Amendment. Like the revenue officers and others who

invaded colonial homes looking for evidence, even though they had no reason to believe the homeowner was guilty of any offense, the Court of Appeals has authorized law enforcement to enter the "cyber-homes" of Rindfleisch and other Wisconsin citizens not suspected of criminal activity, to look for evidence of someone else's wrongdoing.

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

The particularity requirement of the Fourth Amendment is intended to prevent a general exploratory rummaging through a person's belongings. *See Marron v. United States*, 225 U.S. 192, 196 (1927). 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*, 275 U.S. at 196. General warrants do not satisfy the particularity requirement. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). "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).

The warrant applications and affidavits in this case, and the warrants themselves, generally described categories of documents without any particularity as other than a time frame and a relationship to Rindfleisch's email addresses. As such, they 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). Such warrants lack particularity because "'[b]y listing every

type of record that could conceivably be found in an office, the warrant effectively authorized the inspectors to cart away anything they found on the premises.'" *United States v. Leary*, 846 F.2d 592, 602-03 (10th Cir. 1988). Law enforcement officers must be especially careful when seeking authority to seize a broad class of information such as documents or computer data. *Id.*, 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, text messages and other forms of electronic communication.

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

These emails very likely included communications that are clearly privileged under the law, such as communications with her attorneys or physicians, protected under the Sixth Amendment and HIPAA, 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, most of which had no 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.

Despite this extremely broad net requiring Yahoo and Google to produce "all communications," the Court of Appeals affirmed the circuit court's conclusion that the warrants were not overbroad. because law

enforcement officers were only ***authorized*** to search for specific crimes. The circuit court also found no flagrant disregard for the limitations of the warrants. How could there be? The warrants had no limitations. The warrants required production of ***all*** communications, which could have included privileged, non-privileged and irrelevant communications with family members, friends, health care providers, financial planners and even clergy.

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 allowed state investigators to rifle through ***all*** of Rindfleisch's personal, privileged communications without limitations. The conclusion that the warrants were not tantamount to general warrants permitting exploratory rummaging and

excessive searches ignores the history of the Fourth Amendment and the reality of the ever-expanding universe of electronic and digital data. This Court must accept review to address this violation of Rindfleisch's rights under the Fourth and Fourteenth Amendments and their Wisconsin constitutional corollaries.

II. This Court Should Accept Review Because Continuing Advances In Technology Mandate Evolving Considerations And Application Of The Fourth Amendment.

A. This Court Should Accept Review to Establish Protocols For Circuit Courts Presented With Affidavits Seeking Warrants For Electronic And Digital Files And Records.

As noted in the Introduction to this petition, courts across the country have opined whether they should establish protocols for accessing and screening digital data files obtained via search warrants. Many courts, like the Court of Appeals here, saw no need for new protocols, concluding there is no difference between traditional searches of file cabinets and drawers and search of email accounts and other digital

data. *See Rindfleisch*, at ¶21. (App.121). Those conclusions have been cast into doubt by the *Riley* court's expressed recognition of the quantitative and qualitative distinction between physical papers and digital data.

It was that same distinction that led the *Cunnius* court to conclude that courts must reevaluate the application of dated Fourth Amendment law when considering searches and seizures involving technology. Simply put, 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, such searches are not akin to searching drawers in file cabinets:

> 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. In addition, information and data can be removed from a file cabinet and destroyed; digital data cannot. *Id*. at 1146.

The court also noted the vast quantities of information captured via a search of digital files 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.

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.

Therefore, to ensure that the dueling interests of government and its citizens are balanced, the court must establish procedural safeguards:

> … 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).

The *Cunnius* court rejected the government's argument that procedural safeguards were neither necessary nor required, despite the breadth of the warrant requested, and 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.

Unlike the Court of Appeals below, the *Cunnius* court recognized the kinship between warrants authorizing limitless searches of digital files:

> 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.

Another case recognizing the need to establish safeguards or protocols for searching electronic or digital data was *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." *Cunnius*, at 1149-50, *citing CDT III*.

The CDT 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, *quoted in Cunnius*, at 1151.

B. Advances In Technology Require Review Of Wisconsin's Application Of The Fourth Amendment As A Matter Of Public Policy.

As the Supreme Court confirmed in *Riley*, courts must consider what is and is not a "reasonable" search and seizure in the context of the quantitative and qualitative distinctions between papers in a file cabinet and electronically-stored digital data. Technological advances allow government intrusion into the private lives of citizens never contemplated in the wildest dreams of the Framers of the Constitution. In mid-2013, just before Rindfleisch filed her initial brief in the Court of appeals, news broke that the government has been monitoring the mobile devices, social media posts, tweets and blogs of American citizens and generally has used technology to invade the privacy of citizens for no reason other than "to protect national security." A laudable goal – provided this action does not trample the civil liberties of American citizens.

Technology provides opportunities for investigators to invade privacy without leaving any

clues that they snuck into a citizen's "cyber-house" without prior notice. In many cases, this spying is harmless – no one really cares about citizens reading or commenting on celebrities or television shows. But what happens when the websites accessed and comments made are personal and either constitutionally or statutorily privileged?

Concerns over the constitutionality of government monitoring of the personal lives of its citizens are exacerbated when the government authorizes a search warrant for ***all*** communications stored in a citizen's email account. Such broad warrants allow investigators to read private communications between a citizen and his or her lawyer, priest, rabbi, physician, psychiatrist or spouse. They allow access to private medical information intended to be shared only with family and close friends. Absent limits, every bit of personal information ever placed in cyber-space is fair game, despite the Bill of Rights. 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.

To this point, both federal and state laws interpreting the Fourth Amendment and its state corollaries have yet to catch up to the ever-evolving world of the 21st century. The question is whether decades- and even centuries-old Fourth Amendment jurisprudence remains viable in assessing warrants issued for digital information. As technology continues to advance and more individuals, businesses and organizations go "paperless," challenges to the seizure and search of digital records repeatedly will be presented to Wisconsin courts. The orderly administration of justice cries out for this Court to accept review to analyze carefully the Fourth Amendment's application to such records and, ultimately, to reach the same conclusion as the *Cunnius* court.

CONCLUSION

The Court of Appeals' decision upholds the issuance of warrants to search the email accounts of individual citizens without presenting any probable cause that the owner of those records engaged in any criminal activity, authorizing fishing expeditions through all of the email files and records of an individual not even suspected of criminal conduct. Such searches are unreasonable and the Court's decision impermissibly extends the parameters of the Warrants Clause. The state and the courts below believe that so long as a search is "limited" to a denominated email account, investigators are free to open and review every single email related to that account, regardless of content and relationship to any suspected criminal activity. Warrants authorizing law enforcement officers to rummage through private, personal communications without any screening protocols or other checks on the executing officials, are

ripe for the same abuses inherent in general warrants and writs of assistance.

For all of these reasons, defendant-appellant-petitioner Kelly M. Rindfleisch respectfully urges this Court to grant her petition for review, to analyze the right of Wisconsin's citizens to be free from governmental intrusion into their private electronic and digital data without probable cause and, ultimately, to find that the search of Rindfleisch's email accounts violated her constitutional rights and vacate her conviction.

Dated this _____ day of December, 2014.

Respectfully submitted,

GIMBEL, REILLY, GUERIN & BROWN LLP

By:

_____

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

POST OFFICE ADDRESS:

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

CERTIFICATION REGARDING FORM AND LENGTH PURSUANT TO SECTION 809.62.(4)(a), *STATS*.

Pursuant to section 809.62(4)(a), *Stats.,* I certify that this petition conforms to the rules contained in sections 809.19(8)(b) and 809.62(4)(a) for a document produced with a proportional serif font. The length of this petition is 5,485 words.

_____

KATHRYN A. KEPPEL

CERTIFICATION REGARDING APPENDIX PURSUANT TO SECTION 809.62(2)(f), *STATS*.

I hereby certify that filed with this petition, either as a separate document or as a part of this petition, is an appendix that complies with section 809.62(2)(f) and that contains, at a minimum:

> (1) a table of contents;
> (2) the decision of the Court of Appeals
> (3) the findings or opinion of the circuit court; and
> (4) 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 OF ELECTRONIC PETITION PURSUANT TO SECTION 809.62(4)(b), *STATS*.

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

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

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

KATHRYN A. KEPPEL

CERTIFICATION OF ELECTRONIC APPENDIX PURSUANT TO SECTION 809.62(4)(b)), *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