COURT OF APPEALS
DECISION
DATED AND FILED

November 12, 2014

Diane M. Fremgen
Clerk of Court of Appeals

Appeal No. 2013AP362-CR **Cir. Ct. No. 2012CF438**

STATE OF WISCONSIN **IN COURT OF APPEALS**
DISTRICT I

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

KELLY M. RINDFLEISCH,

DEFENDANT-APPELLANT.

APPEAL from a judgment of the circuit court for Milwaukee County: DAVID A. HANSHER, Judge. *Affirmed*.

Before Curley, P.J., Fine and Kessler, JJ.

¶1 KESSLER. J. At issue in this appeal is whether the circuit court erred in denying Kelly M. Rindfleisch's motion to suppress all evidence resulting from a search warrant ordering Internet Service Providers (ISPs) Google and Yahoo to produce emails from Rindfleisch's email accounts with them from

January 1, 2009, until October 10, 2010, together with the account ownership identifying data. Rindfleisch claims the warrants lacked sufficient particularity and thus were "general warrants" in violation of her Fourth Amendment rights. We affirm.

BACKGROUND

¶2 Rindfleisch was charged with four counts of misconduct in public office, in violation of WIS. STAT. § 946.12(3) (2009-10),[1] based on a complaint alleging that she engaged in partisan campaign activities, including political fundraising, during working hours while she was simultaneously a Milwaukee County employee working for then-County Executive Scott Walker. The criminal complaint alleged that during her County work hours, Rindfleisch campaigned for Walker's 2010 gubernatorial campaign, along with the campaign for Lieutenant Governor Candidate Bret Davis.

¶3 The complaint states that Rindfleisch was hired by the County Executive's Chief of Staff, Tim Russell, as a policy advisor for the County Executive in early 2010. Rindfleisch was promoted to Deputy Chief of Staff in March 2010. As a Milwaukee County employee, Rindfleisch was issued a laptop and a County email account. According to the complaint, Rindfleisch used a "non-County issued, personal laptop computer and a non-County, private wireless

[1] WISCONSIN STAT. § 946.12 (2009-10) provides: "Any public officer or public employee who does any of the following is guilty of a Class I felony: … (3) [w]hether by act of commission or omission, in the officer's or employee's capacity as such officer or employee exercises a discretionary power in a manner inconsistent with the duties of the officer's or employee's office or employment or the rights of others and with intent to obtain a dishonest advantage for the officer or employee or another."

All references to the Wisconsin Statutes are to the 2011-12 version unless otherwise noted.

Internet connection supplied by Tim Russell," to work on "projects assigned to her by Russell." Rindfleisch also had two personal email accounts: rellyk_us@yahoo.com and kmrindfleisch@gmail.com. Information found in the emails subject to the warrants showed that both of Rindfleisch's personal email accounts were used for political purposes during County work hours.

¶4 On August 11, 2010, Milwaukee County District Attorney Chief Investigator David Budde submitted an affidavit requesting multiple search warrants relating to political activity conducted by Darlene Wink, the Constituent Services Coordinator for Walker. The affidavit incorporated by reference both an affidavit dated May 14, 2010, in support of a petition to enlarge the scope of the John Doe proceedings[2] investigating various potentially prohibited activities conducted by Walker's aides or appointees during his time as Milwaukee County Executive, and an affidavit dated July 1, 2010, "in support of a Search Warrant for the Yahoo Mail accounts of Darlene Wink." According to the August 11, 2010 affidavit, both of the incorporated affidavits tended to establish that Wink conducted partisan political activity while engaged in her official position as an employee within the Office of Milwaukee County.[3]

[2] A John Doe proceeding is described in, and authorized by, WIS. STAT. § 968.26. It authorizes a judge, at the request of a district attorney, to conduct a secret court proceeding to investigate whether a crime has been committed and if so, by whom. The judge has the power to subpoena witnesses, take testimony, and issue subpoenas and warrants.

The John Doe proceedings were initiated by prosecutors in 2010 to investigate potentially illegal campaign activities conducted by Walker aides, appointees, and employees during his time as Milwaukee County Executive. The May 14, 2010 request to enlarge the scope of the John Doe proceedings was related to "blog posting activity by Darlene Wink as 'rpmcvp' while serving as an employee in the Office of the County Executive."

[3] In May 2012, Darlene Wink resigned from her position shortly after a *Milwaukee Journal Sentinel* reporter "requested Wink's payroll records … to determine whether she was doing political work on county time."

¶5 Shortly thereafter, the John Doe proceedings expanded to include Russell.[4] On August 20, 2010, Budde submitted another affidavit, "principally to search and seize records and information in the form of digital evidence contained on computer workstations issued by Milwaukee County for Tim Russell's use." The affidavit did not refer to, or implicate, Rindfleisch. However, an exhibit to the affidavit included an email from Russell to Rindfleisch, including the email chain to which Russell's email related. The chain included various emails discussing political matters. The email addresses in the chain included Russell's email address, "JillB@scottwalker.org," Rindfleisch's Milwaukee County email account and her Google email account.[5]

¶6 Two months later, on October 20, 2010, Budde submitted another affidavit supporting a search warrant application to require emails between January 1, 2009, and October 20, 2010, from Rindfleisch's Google and Yahoo accounts, and from the email accounts for Russell, Brian Pierick, and "ScottForGov." The affidavit explained that Budde believed the email accounts would contain evidence of Russell's misconduct in public office because emails deleted from Russell's Google account may have remained in Rindfleisch's

[4] Russell was ultimately charged with three counts of theft by embezzlement, contrary to WIS. STAT. § 943.20(1)(b), after then-County Executive Walker designated a nonprofit corporation controlled by Russell to manage the "Operation Freedom" funds used for an annual veterans event run by the Milwaukee County Executive's office. Russell ultimately pled guilty to one of the theft-by-embezzlement counts. His conviction is being appealed in case No. 2014AP451-CR.

[5] It is apparent from the record in this case that the State necessarily followed numerous email trails in the John Doe proceedings to determine the extent of statutorily prohibited political and fundraising activity occurring in government offices and/or on government time. While the record before us suggests that approximately sixteen thousand emails from the identified Rindfleisch accounts were produced by the ISPs in response to the warrants, that is hardly surprising in view of the significant number of people receiving copies and the twenty-two months involved.

accounts. Budde explained why Rindfleisch's email accounts would probably contain evidence of Russell's misconduct:

> While e-mail accounts will often contain many e-mails dating back over months or even years, it is entirely probable that … over time a user can delete 'without a trace' some e-mails held in accounts that are hosted by a provider of electronic communications services. That is to say that e-mails may not be found in the timrussellwi@gmail.com because they have been deleted, but such e-mails may remain in the Rindfleisch [account].
>
> A review of the e-mail threads in this investigation suggest that a number of potentially relevant e-mails have been deleted from the timrussellwi[@]gmail inbox. Evidence from the Rindfleisch accounts will either tend to establish the completeness of the e-mail evidence thus far collected, or it will provide additional evidence of otherwise deleted e-mails. In either event, the evidence from these e-mail accounts will be relevant and valuable.

¶7 The warrants issued to Google and Yahoo on October 20, 2010,[6] were substantially similar. Both contained information identifying the statutory authority of the investigation (the John Doe proceeding), and the identifying email account information for the ISPs. Both warrants required:

> **RECORDS TO BE PRODUCED**: For the time period of January 1, 2009, to the present, this warrant applies to information associated with the account identified as … stored at premises owned, maintained, controlled, or operated by [the ISP at their respective headquarters address]. This warrant requires, **ON OR BEFORE NOVEMBER 22, 2010** the production of:
>
> a. The contents of all communications stored in the [ISP] 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;

[6] The affidavit indicates that the time period involved in the request, namely January 1, 2009, "to the present," i.e. October 20, 2010, was "reasonably related to the current campaign season for the Office of the Governor." Rindfleisch has not argued that the time period involved was unreasonable.

> 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 [the ISP] and any person regarding the accounts, including contacts with support services and records of action taken.

¶8 The warrant issued to Google additionally included the following production request:

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

¶9 Both warrants requested the ISPs to search for evidence of the specific crimes of misconduct in public office and political solicitation involving public officials and employees. The warrants state that the search was to be “for the following evidence of crime”:

> For the time period of January 1, 2009 to the present, all records relating to Misconduct in Public Office and Political Solicitation involving Public Officials and Employees, violations of §§ 946.12, 11.36 and 11.61 of the Wisconsin Statutes, including information relating to the financial or other benefit provided to any private and/or political cause or organization either effected using Milwaukee County facilities or effected during periods of normal county work hours or both.
>
> The terms “records” and “information” include all items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage.

Which objects constitute evidence of the commission of a crime, to wit;

DESCRIBE CRIME OR CRIMES:

(1) Misconduct in Public Office; and

(2) Political Solicitation involving Public Officials and Employees committed in violation of sections 946.12, 11.36[7] and 11.61[8] of the Wisconsin Statutes.

---

[7] WISCONSIN STAT. §11.36 provides:

Political solicitation involving public officials and employees restricted.

(1) No person may solicit or receive from any state officer or employee or from any officer or employee of the University of Wisconsin Hospitals and Clinics Authority any contribution or service for any political purpose while the officer or employee is engaged in his or her official duties, except that an elected state official may solicit and receive services not constituting a contribution from a state officer or employee or an officer or employee of the University of Wisconsin Hospitals and Clinics Authority with respect to a referendum only. Agreement to perform services authorized under this subsection may not be a condition of employment for any such officer or employee.

(2) No person may solicit or receive from any officer or employee of a political subdivision of this state any contribution or service for any political purpose during established hours of employment or while the officer or employee is engaged in his or her official duties.

(3) Every person who has charge or control in a building, office or room occupied for any purpose by this state, by any political subdivision thereof or by the University of Wisconsin Hospitals and Clinics Authority shall prohibit the entry of any person into that building, office or room for the purpose of making or receiving a contribution.

(4) No person may enter or remain in any building, office or room occupied for any purpose by the state, by any political subdivision thereof or by the University of Wisconsin Hospitals and Clinics Authority or send or direct a letter or other notice thereto for the purpose of requesting or collecting a contribution.

(5) In this section, "political purpose" includes an act done for the purpose of influencing the election or nomination for election of a person to national office, and "contribution" includes an act done for that purpose.

(6) This section does not apply to response by a legal custodian or subordinate of the custodian to a request to locate, reproduce or inspect a record under s. 19.35, if the request is processed in the same manner as the custodian or subordinate responds to other requests to locate, reproduce or inspect a record under s. 19.35.

[8] WISCONSIN STAT. §11.61 describes the criminal penalties applied to, and entities responsible for prosecution of, political solicitation involving government employees.

Both warrants allowed the records to be delivered to the District Attorney's office.

¶10 The ISPs complied with the warrants by sending the District Attorney: (1) subscriber identifying information for the provided email address(es); (2) session timestamps and originating IP addresses for logins for the dates requested in the warrant; and (3) CDs containing the emails and contacts lists available to the ISP for the dates requested.[9]

¶11 On October 28, 2010, Google responded to the warrant stating: "To the extent any document provided herein contains information exceeding the scope of your request, protected from disclosure or otherwise not subject to production, if at all, we have redacted such information or removed such data fields." At oral argument, counsel for Rindfleisch stated that on November 1, 2010, the State asked to have the John Doe proceedings expanded to include Rindfleisch. Others were also included in the expanded proceedings. The State requested a search warrant for Rindfleisch's Milwaukee dwelling in West Allis and her Columbia County property. Counsel advised at oral argument that these warrants were executed, with Rindfleisch present, and her personal computer(s) seized. Her counsel also stated that the computer warrants were not being challenged and are not part of this appeal.

¶12 Yahoo responded on November 19, 2010, swearing in an affidavit: "Pursuant to the Federal Stored Communications Act, 18 USC §§ 2701 *et. Seq*., we have redacted information, including removing certain data fields, that exceeds

---

[9] Rindfleisch has not objected to the account ownership information, times and dates of email transmissions, etc. required by the warrants. Consequently, we limit our discussion to her objection to production of the text content of the emails.

the scope of this request, is protected from disclosure or is otherwise not subject to production."

¶13 On January 26, 2012, Rindfleisch was charged with four counts of misconduct in public office. The specific dates[10] of the four alleged offenses were all in the Spring of 2010 (prior to the date of the warrants), and all were supported by electronic evidence. The criminal complaint includes copies of several emails between Rindfleisch and Russell, using her Google and Yahoo accounts. It also identifies multiple chat transcripts between Rindfleisch and other campaign aides. These electronic communications, along with other information in the complaint, indicate that Rindfleisch intentionally engaged in partisan political campaign activities[11] during her Milwaukee County work time.

¶14 Rindfleisch filed a motion to suppress all evidence obtained as a result of the search warrants issued to Yahoo and Google. Rindfleisch argued that the warrants "purportedly permitted by … section 968.375, *Stats.*, eviscerates her privacy rights under the Fourth and Fourteenth amendments and correlative provisions under the Wisconsin Constitution … [and] may well run afoul of Rindfleisch's other constitutional protections, including her rights under the First and Sixth Amendments and HIPPA (*sic*) laws."[12] The focus of Rindfleisch's suppression argument to the circuit court was that: (1) the warrants failed to

[10] The dates of the alleged offenses were April 3, 2010, April 16, 2010, May 3, 2010, and May 4, 2010.

[11] According to a chat transcript referenced in the complaint, Rindfleisch told a friend that her private laptop was on a "separate system," making it possible for her to discuss campaign activities at work. In that same chat transcript, she also told her friend that "half of what I'm doing is policy for the campaign."

[12] Rindfleisch does not develop arguments on appeal which rely on the Fourteenth, First, or Sixth Amendments of the United States constitution, nor on HIPAA laws. Thus those claims are abandoned.

identify the objects to be seized with requisite particularity; and (2) WIS. STAT. § 968.375 is unconstitutional as applied to her case. Rindfleisch argued in her brief supporting her motion that "[t]he warrants required an unknown employee of the ISPs to produce all of their records, and then left it to law enforcement officers to sift through [her] personal, private communications to determine which of those communications actually related to the case…. The ISPs complied with the warrants. Law enforcement officers then had *carte blanche* to rummage through [her] personal electronic communications."

¶15 After briefing and a hearing, the circuit court orally denied Rindfleisch's motion, finding:

> [T]he warrants authorized the search of specific e-mail accounts for a specific time period for specific crimes which evidenced campaign activity by government employees. Even if the warrants were overbroad, I find the items are within the scope of the warrants – or the items within the scope of the warrants should not be suppressed because the search is not conducted in, quote, flagrant disregard for the limitations, end of quote, of the warrant.
>
> Generally items seized within the scope of a warrant need not be suppressed simply because other items outside the scope of the warrant were also seized, unless the entire search was conducted in a flagrant disregard for the limitations of the warrant.

¶16 Rindfleisch subsequently pled guilty to one count of misconduct in public office; the State dismissed the remaining three counts. 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. This appeal is limited by WIS. STAT. § 971.31(10) to the circuit court's denial of Rindfleisch's motion to suppress the evidence obtained from Google and Yahoo.

DISCUSSION

A. Standard of Review.

¶17 "On review of a motion to suppress, [an appellate] court employs a two-step analysis." ***State v. Dubose***, 2005 WI 126, ¶16, 285 Wis. 2d 143, 699 N.W.2d 582. "First, we review the circuit court's findings of fact. We will uphold these findings unless they are against the great weight and clear preponderance of the evidence." ***Id.*** We "'will uphold findings of evidentiary or historical fact unless they are clearly erroneous.'" ***Id.*** (citation omitted). "Next, we must review independently the application of relevant constitutional principles to those facts. Such a review presents a question of law, which we review de novo, but with the benefit of [the analysis] of the circuit court." ***Id.*** (internal citation omitted).

B. Motions to Suppress Evidence.

¶18 When a party moves to suppress evidence based on an alleged Fourth Amendment violation, the proponent of the motion has the burden of establishing that his Fourth Amendment rights were violated. ***State v. Bruski***, 2007 WI 25, ¶20, 299 Wis. 2d 177, 727 N.W.2d 503. The burden of offering evidence at a suppression hearing has been helpfully described by Wayne R. LaFave in *Search and Seizure: A Treatise On The Fourth Amendment*:

> At the hearing on the motion to suppress, who has the burden of proof with respect to the matters at issue? To understand the full significance of this inquiry, it is first necessary to recall that the term "burden of proof" actually encompasses two separate burdens. One burden is that of producing evidence, sometimes called the "burden of evidence" or the "burden of going forward." If the party who has the burden of producing evidence does not meet that burden, the consequence is an adverse ruling on the matter at issue. The other burden is the burden of

> persuasion, which becomes crucial only if the parties have sustained their respective burdens of producing evidence and only when all the evidence has been introduced.

See 6 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment*, § 11.2(b) (4th ed. 2004) (footnotes omitted).

C. The Warrant Clause and General Warrants.

¶19 Rindfleisch argues that her Fourth Amendment rights have been violated because the warrants here are "general warrants," which "lack the level of particularity required to pass constitutional muster." Specifically, Rindfleisch asserts that:

> 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.

(Emphasis added.)

¶20 The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized.*

(Emphasis added.) It is upon this last clause that Rindfleisch bases her entire argument. Specifically, Rindfleisch contends that the warrants at issue lacked sufficient particularity and were unconstitutional general warrants.

¶21 The United States Supreme Court, in ***Steagald v. United States***, 451 U.S. 204 (1981), explained the background and definition of a general warrant:

> The Fourth Amendment was intended partly to protect against the abuses of the general warrants that had occurred in England and the writs of assistance used in the Colonies. *The general warrant specified only an offense* – typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched. Similarly, *the writs of assistance* used in the Colonies *noted only the object of the search*—any uncustomed goods—and thus left customs officials completely free to search any place where they believed such goods might be. *The central objectionable feature of both warrants was that they provided no judicial check on the determination of the executing officials* that the evidence available justified an intrusion into any particular home.

See ***id.*** at 220 (internal citations omitted, emphasis added).

D. The Warrants at Issue did not Violate the Fourth Amendment's Particularity Requirements.

¶22 Typically, when officers exceed the scope of a search warrant, the remedy is to suppress only items seized outside the scope of the warrant. ***State v. Petrone***, 161 Wis. 2d 530, 548, 468 N.W.2d 676 (1991), *overruled on other grounds by* ***State v. Greve***, 2004 WI 69, ¶31 n.7, 272 Wis. 2d 444, 681 N.W.2d 479. However, if the search is conducted in "flagrant disregard" of the limitations in the warrant, all items seized—even items within the scope of the warrant—are suppressed. ***Petrone***, 161 Wis. 2d at 548. When a search is conducted with flagrant disregard for the limitations found in the warrant, the Fourth Amendment's "particularity requirement is undermined and a valid warrant is transformed into a general warrant thereby requiring suppression of all evidence seized under that warrant." ***United States v. Medlin***, 842 F.2d 1194, 1199 (10th Cir. 1988).

¶23 "The United States Supreme Court has interpreted the Warrant Clause to be precise and clear, and as requiring only three things: (1) prior authorization by a neutral, detached [judicial officer]; (2) a demonstration upon oath or affirmation that there is probable cause to believe that evidence sought will aid in a particular conviction for a particular offense; and (3) a particularized description of the place to be searched and items to be seized." ***State v. Sveum***, 2010 WI 92, ¶20, 328 Wis. 2d 369, 787 N.W.2d 317 (citations and quotation marks omitted).

¶24 Keeping in mind the Supreme Court's definition of a general warrant and its interpretation of the Warrant Clause, we measure the warrants at issue against each requirement provided by the Warrant Clause.

1. Prior Authorization by a Neutral, Detached Judicial Officer.

¶25 The warrants were signed on October 3, 2010 by an experienced jurist, Reserve Judge Neal Nettesheim.[13]

2. Demonstration by an Oath or Affirmation that there is probable cause to believe that the evidence seized will lead to a particular conviction of a particular offense.

¶26 David E. Budde, the Chief Investigator assisting the John Doe Judge, swore to an affidavit in support of both the Google warrant and the Yahoo warrant. His affidavit contained numerous pages of detailed information, along with multiple exhibits.

[13] Judge Nettesheim served as a Circuit Court Judge from 1975 to 1984. He served as a Court of Appeals Judge from 1984 until his retirement in 2007. He was appointed by the Wisconsin Supreme Court to preside over the John Doe proceeding in which he issued the warrants in question.

¶27 The affidavit stated the warrants request related "to violations of Wisconsin Statutes § 964.12, Misconduct in Public Office, by Milwaukee County employee Timothy Russell of the Department of Health and Human Services (and formally of the Milwaukee County Executive's Office)." The affidavit explained that "county desktop computers used by Tim Russell were seized pursuant to search warrants" in this investigation, and forensic examination of those computers revealed fragments of Yahoo messages between Russell's Yahoo account and Rindfleisch's rellyk_us@yahoo.com account. In addition, emails obtained by search warrant from Russell's Google account "indicate[] that on numerous occasions, Rindfleisch forwards messages from her Milwaukee County e-mail account … to a private e-mail account at kmrindfleisch@gmail.com. In turn, … [Rindfleisch] sends those messages on to additional parties, including Tim Russell and persons associated with the Scott Walker campaign." The affidavit stated that "[m]any of these e-mails were sent during presumptive business days, Monday through Friday between 8 a.m. and 5 p.m." In addition, emails contained in Russell's timrussellwi@gmail.com account show he received a number of emails from Rindfleisch using rellyk_us@yahoo.com.

¶28 In a fact scenario similar to the case at bar, the United States Court of Appeals for the Ninth Circuit, in ***United States v. Adjani***, 452 F.3d 1140 (9th Cir. 2006), concluded that a search warrant to search the electronic files of Jana Reinhold passed constitutional muster. In that case, the government applied for a warrant to search Reinhold's electronic files based on her connection to Christopher Adjani. ***Id.*** at 1142. Adjani was suspected of threatening to sell confidential payment information from Paycom Billing Services. ***Id.*** at 1143. Based in part on email communications discovered between Adjani and Reinhold, both were charged with conspiring to commit extortion and transmitting a

threatening communication with intent to extort. ***Id.*** at 1142. Both Adjani and Reinhold moved to suppress specific emails between them, discovered via Reinhold's personal hard drive, arguing that the warrant lacked probable cause because the warrant did not label Reinhold as a suspect. ***Id.*** at 1146-47.

¶29 In a decision reversing the federal district court, the Ninth Circuit concluded that the warrant stated sufficient probable cause because the warrant was only required to establish probable cause to believe that evidence of the crimes at issue could be found on Reinhold's hard drive, regardless of whether Reinhold was a suspect. ***Id.*** at 1147.[14]

¶30 Likewise, the warrant at issue in this case established, in no uncertain terms, that the State sought evidence of two particular crimes—misconduct in public office and political solicitation involving public officials and

[14] The Dissent appears to be of the view that because the affidavits supporting the email searches did not establish probable cause to believe *Rindfleisch* had committed a crime, the warrants violated her Fourth Amendment rights. *See* Dissent, ¶45.

The error in the Dissent's analysis is evident upon review not only of the United States Court of Appeals decision discussed above, but more compellingly upon review of the United States Supreme Court's opinion in ***Zurcher v. Stanford Daily***, 436 U.S. 547 (1978), where the Supreme Court explained:

> The Warrant Clause speaks of search warrants issued on "probable cause" and "particularly describing the place to be searched, and the persons or things to be seized." In situations where the State does not seek to seize "persons" but only those "things" which there is probable cause to believe are located on the place to be searched, there is no apparent basis in the language of the Amendment for also imposing the requirements for a valid arrest—probable cause to believe that the third party is implicated in the crime.

Id. at 554. The Court also observed that "the State's interest in enforcing the criminal law and recovering evidence is the same whether the third party is culpable or not." ***Id.*** at 555. Here, the affidavits established probable cause to believe that *Russell* had committed a crime, and probable cause to believe that evidence of *Russell's* crime probably could be found on emails Rindfleisch had sent to or received from Russell. More is not required by the Fourth Amendment.

employees. The warrant requested the production of the following items, as material to this case, to establish evidence that the two particular crimes at issue were committed by Russell:

- Additional email accounts discovered by the investigation which appear to be controlled by Russell;
- Accounts controlled by Rindfleisch, the current Deputy Chief of Staff in the Milwaukee County Executive's Office, which accounts are believed to contain evidence in the form of emails sent to and received by Russell; and
- Accounts controlled by Russell's roommate, Brian Pierick, which were believed to have evidence of Russell's political activity while Russell was serving as a Milwaukee County employee.

¶31 Like in ***Adjani***, the warrants at issue in this case sought items based on the probable cause to believe that specific crimes were committed. The scope was limited to evidence of misconduct in public office or political solicitation involving public officials and employees, in violation of WIS. STAT. §§ 946.12, 11.36, and 11.61.

3. Particularized description of the place to be searched and the items to be seized.

¶32 The two ISPs, Google and Yahoo, were specifically identified by name and address. The places within their data storage system were particularly described as "For the time period of January 1, 2009, to the present, this warrant applies to information associated with the account identified [in the warrant] stored at premises owned, maintained, controlled, or operated by" the particular

ISP. Rindfleisch has offered no evidence suggesting that the search exceeded the locations here described.

¶33 As to the items to be seized, the affidavit identified specific email accounts—four with Yahoo and two with Google—with which the warrants were concerned. Two were accounts in Russell's name: tdrussell63@yahoo.com, and trussell@yahoo.com. One account was in Pierick's name, bpierick@yahoo.com. Two of the accounts were in Rindfleisch's name: rellyk_us@yahoo.com and kmrindfleisch@gmail.com. One account, scottforgov@gmail.com, was an account that Budde believed was actually controlled by Pierick, who was also a blogger for the Walker campaign.

¶34 Additionally, as we have seen, information held by the ISPs which specifically identified the owner of the accounts and the personal contact information associated with the accounts, was also requested. This was necessary to ensure that the accounts were not actually owned or controlled by someone other than the suspected owner.

¶35 Rindfleisch has offered no evidence suggesting that information beyond those requests was produced.

E. The ISPs returned their Electronic Information with an Oath or Afirmation that the Records Produced Complied with the Warrant.

¶36 As noted, when Google responded to the warrant, it stated:

> To the extent any document provided herein contains information exceeding the scope of your request, protected from disclosure or otherwise not subject to production, if at all, we have redacted such information or removed such data fields.

When Yahoo produced its records, it swore in an affidavit that:

> Pursuant to the Federal Stored Communications Act, 18 USC §§ 2701 et. Seq., we have redacted information, including removing certain data fields, that exceeds the scope of this request, is protected from disclosure or is otherwise not subject to production.

¶37 The Dissent relies on ***United States v. Ganias***, 755 F.3d 125, 134-135 (2d Cir. 2014), for the well-established general proposition that "The government is barred from accessing data not within the scope of the search warrant." *See* Dissent, ¶44 In ***Ganias***, federal agents made forensic mirror images of Stavros Ganias's hard drives. ***Id.*** at 128-29. The record in ***Ganias*** included findings that the agents knew they could not have access to the information on the hard drive image not covered by the warrant, and that they carefully separated the covered information from that not covered. ***Id.*** at 137-38. However, instead of returning the information from the hard drive image not covered by the warrant, the government kept it. ***Id.*** at 138. Three years later, another government agency used the improperly retained hard drive image to bring charges against the defendant. ***Id.*** at 130. Predictably, that did not sit well with the court, which noted extensive facts in the record amounting to obvious government misconduct. ***Id.*** at 137-40. The record before this court permits no such findings. The ISPs asserted that they had complied with the warrant, and even that they had redacted information from their productions. Rindfleisch has not produced a shred of evidence to dispute those representations, has rejected the opportunity before this court to identify specific documents that she claimed were beyond the scope of the warrant, and has relied instead on rhetorical salvos attacking the entire scope of the warrants.

F. More is not required here by the Fourth Amendment simply because the Evidence seized is Electronic Data.

¶38 Rindfleisch urges this court to adopt the protocol described in ***In the Matter of the United States Of America's Application For A Search Warrant To Seize And Search Electronic Devices From Edward Cunnius***, 770 F. Supp. 2d 1138 (W.D. Wash. 2011),[15] a memorandum order by a federal magistrate judge. In that case, Edward Cunnius was suspected of selling counterfeit Microsoft technology. ***Id.*** at 1139. The government applied for a search warrant to search, among other things, all of Cunnius's electronically stored information. ***Id.*** at 1139-1140. The magistrate judge found the requested warrant overbroad because the warrant made no reference to the use of a filtering agent to sort through all of the electronic evidence. ***Id.*** at 1141.

¶39 Rindfleisch argues, based on ***Cunnius***, that the Fourth Amendment, as applied to electronic communications, should be read to require an extra layer of protection not historically accorded paper documents, namely an electronic "filter" (the details of which she does not specify) to keep her "personal" or "private" material from being disclosed. She has identified no specific "personal" or "private" material that has been improperly produced. Alternatively, still based on ***Cunnius***, she suggests that a third party should have been appointed by the warrant-issuing judge to review what Google and Yahoo produced. That third person would be the arbiter of what, within the data produced, would be available to the government. We are not persuaded.

[15] As of the writing of this opinion, the only cases that have considered ***In the Matter of the United States Of America's Application For A Search Warrant To Seize And Search Electronic Devices From Edward Cunnius***, 770 F. Supp. 2d 1138 (W.D. Wash. 2011), have declined to follow it.

¶40 The Fourth Amendment parameters of search and seizure law, largely developed in the context of obtaining tangible evidence, are not necessarily inapplicable to all searches for and seizures of electronic information. For example, a search warrant for a filing cabinet, located in a particular place, which contains a year's worth of correspondence between, or relating to, two particular individuals, would normally be searched where the filing cabinet is located by the officers executing the warrant. Likewise, many documents in that filing cabinet would have nothing to do with either of those individuals. The only way the officer could distinguish between what relates to either of those individuals and what does not, is to look through all of the documents in the filing cabinet. Law enforcement officers have long had to separate the documents as to which seizure was authorized from the other documents. So far, as we have been able to discover, that necessity has not turned an otherwise valid warrant into a "general" warrant. We see no constitutional imperative that would change the result simply because the object of the search is electronic data from a specific electronic file, for a reasonably specific period of time, in the custody of a specific ISP.

¶41 Further, in this case, both ISPs stated in writing essentially the same thing: that they provided *only* what was required by the warrant, and they removed electronic data beyond the scope of the warrant. Rindfleisch had the opportunity before the circuit court to identify specifically what evidence she believed was improperly seized. She elected not to do so, and instead argued that the warrant on its face did not satisfy the Fourth Amendment.[16]

[16] Rindfleisch moved to seal the documents in the record. Third-party media entities moved to intervene to oppose the motion. We allowed the third-party entities to intervene and asked Rindfleisch to identify which documents she wished to seal as being beyond the scope of the warrants. Rindfleisch, through counsel, declined to do so, asserting that such a search would be too time-consuming and expensive.

CONCLUSION

¶42 Rindfleisch has failed to present any evidence at any time during these proceedings that tends to suggest that her Fourth Amendment rights were violated by the seizure authorized in these warrants. We have concluded that the State established, as the circuit court found, that the warrants in question were based on probable cause established by affidavit, were authorized by a judge, and particularly described the place to be searched and items to be seized. We therefore conclude, as did the circuit court, that the warrants at issue satisfy all of the requirements of the Fourth Amendment. We further find no evidence in this record suggesting in any way that the ISPs provided information beyond the scope of the warrant, much less that the information produced was in flagrant disregard of the scope of the warrant. Consequently, the circuit court's refusal to suppress everything obtained by the State from the ISPs was properly denied.

By the Court.—Judgment affirmed.

Recommended for publication in the official reports.

¶43 FINE, J. (*dissenting*). 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.

A. *Search.*

¶44 We are bound by the Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Supreme Court has explained:

> The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one "particularly describing the place to be searched and the persons or things to be seized." The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. Thus, the scope of a lawful search is "defined by the object of the search and the places in which there is probable cause to believe that it may be found."

Maryland v. Garrison, 480 U.S. 79, 84 (1987) (quoted sources and footnote omitted). Yet, the Majority eschews the Fourth Amendment's command and permits the government to rummage through Kelly Rindfleisch's digital files for

evidence of *her* crime even though the search warrants sought evidence in those files of *another's crime by another person* (Tim Russell) and lacked probable cause to believe that Rindfleisch's digital files had *any* evidence of *any* crime that Rindfleisch might have committed. *See* ***Arizona v. Gant***, 556 U.S. 332, 345 (2009) (The Framers were "concern[ed] about giving police officers unbridled discretion to rummage at will among a person's private effects.") (footnote omitted).

> The Fourth Amendment guards against this practice by providing that a warrant will issue only if: (1) the Government establishes probable cause to believe the search will uncover evidence of a *specific* crime; and (2) the warrant states with particularity the areas to be searched and *the items to be seized*. The latter requirement, in particular, "makes general searches ... impossible" because it "prevents the seizure of one thing under a warrant describing another." This restricts the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item not described in the warrant.

United States. v. Ganias, 755 F.3d 125, 134–135 (2d Cir. 2014) (emphasis added, quoted sources and citations omitted; ellipses in ***Ganias***) (The government is barred from accessing data not within the scope of the search warrant.). Contrary to this enshrined Fourth-Amendment law, the search warrants for Rindfleisch's digital files did not:

- set out probable cause that Rindfleisch had done anything wrong (as the Fourth Amendment requires); and
- describe any place where any evidence that she had done anything wrong could be found (as the Fourth Amendment also requires).

The danger in this type of case is palpable:

> [B]ecause there is currently no way to ascertain the content of a file without opening it and because files containing evidence of a crime may be intermingled with millions of innocuous files, "[b]y necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there." Once the government has obtained authorization to search the hard drive, the government may claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant. There is, thus, "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches.

United States v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013) (quoted sources omitted; second set of brackets in ***Galpin***). Rindfleisch's lawyer told us at oral argument that of the approximately 16,000 documents received from the Rindfleisch email accounts pursuant to the search warrants "there were probably" fewer "than 500 pieces of paper that had Kelly Rindfleisch's political involvement in them." The State thus hardly "inadvertently" stumbled on the ream of pages that led to Rindfleisch's charges. *See* ***Coolidge v. New Hampshire***, 403 U.S. 443, 469–470 (1971) (The "plain view" doctrine does not apply to the government's discovery of implicating material that is not covered by a search warrant if the discovery was not "inadvertent.").

¶45 The Fourth Amendment prohibits the government to legitimately go into a person's voluminous files looking for evidence that *someone else* may have violated the law (here, Russell, the search warrants' object), and then root around those voluminous files to see if the subpoenas' subject (here Rindfleisch) may have also violated the law. Yet, the State admits in its brief that it did precisely

that: "As the warrants and supporting affidavit make clear, however, the John Doe investigation had targeted Tim Russell, not Rindfleisch, and the warrants sought Rindfleisch's communications for the purpose of filling gaps in Russell's e-mail communications." Also, the State was asked at oral argument:

> Court of Appeals Judge: "But there was no probable cause stated in the affidavits [in support of the search warrants] to believe under the Fourth Amendment that Ms. Rindfleisch was guilty of a crime."
>
> Assistant Attorney General: "Right. At that point. … As far as I know they [the prosecutors] did not have any belief that Ms. Rindfleisch or anybody else that was engaged in this kind of conduct [other than Russell, whose emails in Rindfleisch's accounts were sought by the search warrants]. That [Rindfleisch's alleged culpability] became apparent after they [the prosecutors] got the return on the warrant for the documents that were within the scope of the warrant[s] that were approved [namely, for the search of Russell's emails in Rindfleisch's digital accounts]."

(Formatting modified.) The search of Rindfleisch's voluminous digital files was illegal because the search warrants were silent as to whether there was probable cause to believe that she was culpable.

B. *Suppression.*

> Even where a search or seizure violates the Fourth Amendment, the Government is not automatically precluded from using the unlawfully obtained evidence in a criminal prosecution. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Suppression is required "only when [agents] (1) ... effect a widespread seizure of items that were not within the scope of the warrant, and (2) do not act in good faith."
>
> The Government effects a "widespread seizure of items" beyond the scope of the warrant when the Government's search "resemble[s] a general search." Government agents act in good faith when they perform

> "searches conducted in objectively reasonable reliance on binding appellate precedent." When Government agents act on "good-faith reliance [o]n the law at the time of the search," the exclusionary rule will not apply. "The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance."

Ganias, 755 F.3d at 136–137 (quoted sources and citations omitted, brackets and ellipses in ***Ganias***). Here, the exclusionary rule thus applies because: (1) the State both widely and knowingly exceeded the scope of the Rindfleisch search warrants that sought only the Russell emails, and (2) the State did not objectively act in good faith based on Fourth-Amendment law that was clear at the time of the search.

C. *Conclusion*.

¶46 The Majority legitimizes a general warrant and nullifies our Constitution. I respectfully dissent and would grant Rindfleisch's motion to suppress the data provided pursuant to the search warrants that concerned Rindfleisch and not Russell. *See* ***State v. Petrone,*** 161 Wis. 2d 530, 548, 468 N.W.2d 676, 682–683 (1991) ("The general rule is that items seized within the scope of the warrant [here, relating to Russell] need not be suppressed simply because other items outside the scope of the warrant [here, relating to Rindfleisch] also were seized, unless the entire search was conducted in 'flagrant disregard for the limitations' of the warrant.") (footnotes omitted, brackets supplied).