STATE OF MINNESOTA

IN SUPREME COURT

A22-0468

Court of Appeals

Thissen, J.
Concurring, Anderson, Thissen, JJ.
Took no part, Procaccini, J.

State of Minnesota,

Respondent,

vs.

Filed: May 8, 2024
Office of Appellate Courts

Kristi Dannette Mcneilly,

Appellant.

Keith Ellison, Attorney General, Saint Paul, Minnesota; and

Mary F. Moriarty, Hennepin County Attorney, Adam E. Petras, Assistant County Attorney, Minneapolis, Minnesota, for respondent.

Robert D. Richman, St. Louis Park, Minnesota, for appellant.

Paul Sellers, Minnesota Legal Defense, Minneapolis, Minnesota; and

Jill Brisbois, The JAB Firm, Minneapolis, Minnesota, for amicus curiae Minnesota Association of Criminal Defense Lawyers.

Cathryn Middlebrook, Chief Appellate Public Defender, William Ward, Minnesota State Public Defender, Saint Paul, Minnesota, for amicus curiae Minnesota Board of Public Defense.

Edward R. Shaw, Edward R. Shaw, P.A., Brainerd, Minnesota, for amicus curiae National Association of Criminal Defense Lawyers.

Scott M. Flaherty, Taft Stettinius & Hollister LLP, Minneapolis, Minnesota, for amicus curiae Tony Webster.

S Y L L A B U S

1. Search warrants authorizing seizure and search of electronic devices were sufficiently particular under the Fourth Amendment to the United States Constitution and Article I, Section 10, of the Minnesota Constitution.

2. The guilty verdict in this case was surely unattributable to the evidence obtained from the search of a law office and so we need not decide whether the warrants to search that law office were executed in an unreasonable manner because any error in the evidence's admission was harmless beyond a reasonable doubt.

3. When searching the law office of an attorney who is suspected of a crime, specific procedures to safeguard privileged materials are required under the supervisory powers of the Minnesota Supreme Court.

Affirmed.

O P I N I O N

THISSEN, Justice.

An attorney, Kristi McNeilly, was convicted of theft by swindle. During the investigation that led to her conviction, law enforcement executed two warrants—the first to search her law office (the "office warrant") and the second to search the electronic devices seized from her office (the "device warrant"). McNeilly argues that the office warrant was not sufficiently particular under the Fourth Amendment to the United States

Constitution and Article I, Section 10, of the Minnesota Constitution because it allegedly authorized an unlimited search of her electronic devices. She also argues that the device warrant was not sufficiently particular. Finally, she argues that both warrants were executed in an unreasonable manner under the Fourth Amendment and Article I, Section 10, because insufficient procedural measures were taken to safeguard privileged attorney-client communications and attorney work product.

For the reasons discussed below, we hold that the warrants were sufficiently particular. We further conclude that even if we determined that the search warrants were executed in an unreasonable manner in violation of the Fourth Amendment or Article I, Section 10, McNeilly is not entitled to a new trial because, under our governing standard, the jury's verdict was surely unattributable to the district court's decision not to suppress evidence obtained in the search. Consequently, the alleged constitutional error here was harmless beyond a reasonable doubt. Thus, we do not decide whether the searches of McNeilly's office and electronic devices were executed in an unreasonable manner under the Fourth Amendment or Article 1, Section 10. But given our concern about the constitutional and other implications of allowing the police to gain access to privileged attorney-client communications and work-product materials, we use our supervisory powers to establish prospective procedural safeguards for searching the law office of an attorney who is suspected of a crime. We affirm McNeilly's conviction.

FACTS

Attorney Kristi McNeilly swindled a client, M.W., out of $15,000. In May of 2018, M.W. owned a townhouse in Minnetonka where he lived with J.S. (his then-boyfriend) and

two renters. On May 1, 2018, a detective from the Minnetonka Police Department (the "Minnetonka detective"), working with the Southwest Hennepin Drug Task Force, executed a search warrant at the townhouse.[1] During the search, police found a vial of suspected drugs in M.W.'s safe, marijuana in J.S.'s possession, and methamphetamine in the possession of one of the renters. J.S. received a citation, the renter was arrested for methamphetamine possession, and although M.W. was not charged, the vial of suspected drugs was sent by law enforcement to a lab for testing.

At the time of the townhouse search, McNeilly was representing M.W. in a landlord-tenant dispute. M.W. and J.S. met with McNeilly to discuss the existing and potential criminal charges. At the meeting, McNeilly informed M.W. that she had spoken to someone at the prosecutor's office who indicated that they were building a significant case against him. M.W. signed a retainer agreement with McNeilly and paid her $20,000 as required by the agreement. J.S. signed a separate, flat-fee retainer agreement and M.W. also paid that retainer fee.

The Minnetonka detective visited the home of M.W. in early July 2018. Following McNeilly's advice, M.W. did not reveal what the substance in the seized vial was. Several months later, on October 29, 2018, McNeilly represented J.S. at a hearing regarding the marijuana possession; J.S. paid a $200 ticket for a paraphernalia citation. By November 5, 2018—more than 6 months after M.W.'s home was searched—M.W. had not been charged with an offense.

---

[1] The validity of this warrant is not at issue in this case.

McNeilly Proposes that M.W. Make Payment in Return for Leniency

M.W. and J.S. testified that, on November 5, 2018, McNeilly communicated with M.W., stating that it was urgent that they speak. McNeilly claimed that the Minnetonka detective and the prosecutor had asked to meet with her, which she suggested was a bad sign. A few hours later, McNeilly arrived at M.W.'s house and told M.W. and J.S. that she had been invited into the "back room," where esteemed attorneys had the privilege to meet with authorities to make deals for clients that would not involve any charges. She described this as a big step in her career that meant she had "made it."

According to M.W. and J.S., McNeilly claimed that a federal bug had been planted in M.W.'s house by a renter and subsequently removed by the Minnetonka detective when he spoke with M.W. in July. McNeilly claimed that M.W. faced 15–20 years in federal prison, but he could avoid charges if he paid $35,000 to the police union and acted as a confidential informant. McNeilly showed M.W. a copy of a confidential informant form. When M.W. said he did not want to be an informant, McNeilly offered him a second option: pay $50,000 to the police union and no service as a confidential informant would be necessary. M.W. would pay McNeilly and she would deliver the money to the union.

M.W. agreed to the $50,000 option and indicated that he could pay $15,000 that day and the remainder in the next few months. McNeilly said she would have to check with the Minnetonka detective. She went to the garage—ostensibly to make a phone call—and emerged 5–10 minutes later claiming that he had agreed to the deal but that she would be on the hook for the remaining $35,000 if M.W. failed to pay. She also said that the money had to be transmitted to the union by 6 p.m. that same day. McNeilly drove M.W. to the

bank and stood behind him while he got a $15,000 cashier's check. She instructed him to write on the memo line "legal fees." M.W. handed McNeilly the cashier's check, which she immediately deposited into her account. M.W. testified that within a few days, he began to question this arrangement.

McNeilly claims that M.W. and J.S. fabricated this version of events. At trial, she maintained that the $15,000 was payment for legal services.

M.W. contacted Robert Paule, a criminal defense attorney. M.W. retained Paule on his drug case and Paule reached out to the authorities regarding the bribery allegations. Paule advised M.W. to request a refund from McNeilly, ask for receipts, and request his file.

M.W. emailed McNeilly three times asking for a refund of the $15,000. McNeilly refused his request each time. Notably, in response to M.W.'s first request, McNeilly sent M.W. a text stating, "Yes, I got your email. It was paid as directed. So how can I get a refund? This is a serious issue." After the third email, McNeilly responded, "I'm not sure what game you are playing or what you are doing, but I am done playing this. Please stop contacting me." M.W. provided these emails to law enforcement (they were not obtained in the subsequent search of McNeilly's office).

M.W. was charged in January 2019 and ultimately convicted of fifth-degree drug possession. Because of his clean record—and contrary to McNeilly's claims of a massive federal case being built against him—he was offered diversion and no jail time, and upon completion of the diversion process, his felony conviction was expunged.

The Police Investigate McNeilly

The Minnetonka Police Department referred the investigation to the Burnsville Police Department to avoid conflicts during what initially appeared to be a bribery investigation. The Minnetonka detective was placed on administrative leave but was reinstated less than a week later when the department determined that he was not involved in a bribery scheme. Burnsville police interviewed M.W., J.S., and the Minnetonka detective. They also reviewed the detective's phone records and found no calls between him and McNeilly.

Burnsville police obtained a warrant for McNeilly's bank records; the records showed a $15,000 check from M.W. was deposited but there were no subsequent transfers or withdrawals of $15,000.[2] McNeilly spent the money on normal personal expenses. Police also reviewed McNeilly's phone records. The records showed multiple communications with M.W. on November 5, 2018, but no calls between the Minnetonka detective and McNeilly at any time. There was no evidence that the Hennepin County Attorney's Office was engaged in a bribery scheme.

M.W. attempted to get his file from McNeilly by sending a certified letter to the office where he had first met her. The letter was returned because by that point, McNeilly was working from her home office in Woodbury, Minnesota. Paule also tried to get a copy of the file by sending letters to two other office addresses listed for McNeilly online—one in Saint Paul, the other in Minneapolis—but these letters were returned as well. M.W. did

---

[2] The validity of this warrant is not at issue in this case.

not receive his file from McNeilly and no money was returned to him. M.W. provided to police text and email communications with McNeilly.

The Search of McNeilly's Office

After M.W. and Paule were unable to obtain M.W.'s file, police sought and obtained a search warrant for McNeilly's home law office. The office warrant authorized a search of McNeilly's home for "Documents showing occupancy"; "Digital pictures prior to and during the search"; "Computers such as laptops, desktops, and or [sic] towers"; "Electronic devices which could contain or access files held remotely"; "Mobile phone associated with [McNeilly's phone number]"; "Confidential Informant form"; "Any files, invoices, or Documents associated with representation of M.W. and J.S."; and "Retainer agreement for M.W."

Although the affidavit submitted in support of the warrant application indicated that the police would not "do an initial preview" of any computers and would obtain a separate warrant to search those devices, that restriction was not included in the office warrant.

On February 27, 2019, at about 11 a.m., eight or nine officers executed the office warrant. McNeilly was not home during the search. Officers were instructed to seek only information related to M.W. and J.S.; items not pertaining to those clients were to be set aside because they were not supposed to "document anyone's name or retain[] that information." They reviewed invoices and retainer agreements of various clients "to determine whether or not they pertained to" M.W. or J.S. Police seized M.W.'s physical file and various electronic devices including thumb drives, a desktop computer, and a laptop. As is standard practice, police left a notice which included a list of items seized.

The Search of McNeilly's Electronic Devices

On March 5, 2019, police applied for and obtained a second search warrant—the device warrant—authorizing a search of the electronic devices police had seized. The device warrant was not limited to a specific suspected crime or time frame, but the warrant was limited to searching for the following specific items: "Files related to communications, calendar events, invoices, retainer agreements, casefiles, and documents pertaining to M.W. and J.S."; "Calendar events, communications, or documents showing contact with [the Minnetonka detective]"; "Confidential Informant form"; and "Any files or notes associated with representation of M.W. and J.S."

The warrant application requested that the Dakota County Electronic Crimes Task Force (the "Task Force") be authorized to search the devices. The Task Force is organized under the Dakota County Sheriff's Office and includes personnel from various police departments, including one detective from the Burnsville Police Department. The Burnsville Police Department sends all of its computer forensic work to the Task Force.

The application also proposed that files be provided to Burnsville police only after the Task Force reviewed the files and determined which ones were "important to this investigation." The warrant did not include any such limitation. Rather, the second warrant included what appears to be boilerplate language authorizing a variety of persons to search

the seized devices, including "peace officers of the State of Minnesota, and any other authorized person"—categories that would include the Burnsville police.[3]

A civilian forensic examiner who works for the Task Force reviewed the files for relevancy. The examiner was not an attorney. She was given a starting list of search terms including the full names of M.W., J.S., and the Minnetonka detective, as well as the term "CI form." Burnsville police did not obtain an explicit waiver of attorney-client privilege from M.W. or J.S. No additional steps were taken to filter out privileged information.

In conducting the search, the examiner started with search terms that yielded results allowing her to view the words directly surrounding the term. She then looked at the file name to determine whether the file related to the investigation. If the PDF's file name included a client name other than M.W. or J.S., the examiner did not open the file. She manually opened some PDF documents because those files were not otherwise searchable. She immediately closed the document if it was unrelated to the investigation.

The examiner found and provided to the Burnsville Police Department a number of documents which she deemed relevant. No comprehensive log of the documents searched by the examiner or the documents provided to the Burnsville Police Department is in the record. The record does show that the documents provided included documents pertaining to M.W.'s housing court matter, search warrant returns pertaining to the Minnetonka

---

[3] The device warrant did not describe a search *process* at all. It merely listed the devices to be searched, where those devices were located, the items the police were seeking, and the persons authorized to conduct the search. It stated that probable cause existed for the search and concluded that the authorized people "are hereby commanded to enter and search between the hours of 7 a.m. and 8 p.m., to search the above-described devices(s) for the described property and thing(s) . . . ."

detective, QuickBooks entries in M.W.'s name, invoices associated with M.W., an electronic folder in M.W.'s name, a document downloaded on November 5, 2018, with the heading "Texas Alcoholic Beverage Commission Confidential Informant-Agreement of Understanding," and a second document—created on November 5, 2018—that was identical except for a modified heading which stated, "Southwest Hennepin Drug Task Force Confidential Informant-Agreement of Understanding."

Court Proceedings

On March 5, 2019, the same day Burnsville police applied for and obtained the device warrant, McNeilly initiated a civil suit and then brought a motion requesting a district court order returning her client files and seeking "relief from the search of [her] office and seizure of perhaps a thousand client files." *In re K.M.*, 940 N.W.2d 164, 168 (Minn. 2020) (internal quotation marks omitted) (quoting McNeilly's motion in the case). Following an ex parte hearing pursuant to Minn. Stat. § 626.04(a) (2022), the court denied McNeilly's motion, holding that "the seized property is being held in good faith as potential evidence in a matter that is uncharged at this time." *K.M.*, 940 N.W.2d at 169 (internal quotation marks omitted (quoting district court order). On March 13, 2019, McNeilly filed a petition for a writ of prohibition in the Minnesota Court of Appeals. On March 26, 2019, the court of appeals denied relief. *K.M. v. Burnsville Police Dep't*, No. A19-0414, Order at 4 (Minn. App. filed Mar. 26, 2019).

On June 10, 2019, McNeilly was charged with theft by swindle in violation of Minnesota Statutes section 609.52, subdivision 2(a)(4) (2022).[4] It is this criminal proceeding that is before us on appeal.

Meanwhile, in the ongoing civil case, McNeilly filed a petition for review of the denial by the court of appeals of the writ of prohibition. We granted the petition but ultimately denied relief. Our decision was limited to holding that, under Minn. Stat. § 626.04(a), the State did not need to return McNeilly's client files and we stated that the State should have provided McNeilly copies of those files. *K.M.*, 940 N.W.2d at 169, 172. With respect to the constitutional claims, we noted the "many concerns" raised by "searches of offices of attorneys targeted in criminal investigations," but held that the limited factual record presented by the expedited proceeding was not the appropriate occasion to announce guidelines for how such searches are conducted consistent with the Minnesota and United States Constitutions. *Id.* at 171. We emphasized that our decision was without prejudice to raising those issues in the pending criminal case. *Id.* at 172.

With the civil case resolved, McNeilly moved—in this criminal proceeding—to suppress the evidence gained from the searches. The district court held an evidentiary hearing on that motion, denied relief, and concluded that the search of McNeilly's client files were not unreasonable because the police used "a significant amount of care."

---

[4] The statute provides that "[w]hoever does any of the following commits theft . . . (4) by swindling, whether by artifice, trick, device, or any other means, obtains property or services from another person." Minn. Stat. § 609.52, subd. 2(a)(4).

The Trial and Appeal

McNeilly's case was tried and documents seized in the searches of her law office and computers were introduced by the State at trial, specifically:

- A retainer agreement dated May 15, 2018, for M.W.'s drug matter.
- Invoices for payments from M.W. to McNeilly.
- The Fake Confidential Informant Agreement.
- A Texas Confidential Informant Agreement.

Much of the evidence used at trial, however, was not obtained from the searches of McNeilly's office and computer. The evidence unrelated to the office and computer searches included bank records, phone records, text messages and emails between McNeilly and M.W., as well as testimony from M.W., J.S., Paule, and several members of law enforcement. McNeilly has never identified any privileged communications or work-product material that were introduced into evidence.[5]

McNeilly was convicted and sentenced to 366 days in prison, with a 3-year stay of the sentence. She appealed her conviction, and the court of appeals affirmed. *State v. Mcneilly*, No. A22-0468, 2022 WL 17747792, at *4 (Minn. App. Dec. 19, 2022).

We granted McNeilly's petition for review.

ANALYSIS

On appeal, McNeilly asserts that both the office warrant and the device warrant were insufficiently particular. She also claims that the execution of the search warrants was

[5] McNeilly does not assert that the confidential informant forms are privileged or work product.

constitutionally unreasonable because the police did not adequately safeguard the attorney-client and work-product privileges. We address these arguments in turn. We also establish, under our supervisory powers, required procedures to safeguard privileged materials in future searches of law offices of attorneys suspected of a crime.

I.

A.

We review a district court's ruling on the constitutionality of a search or seizure de novo. *State v. Anderson*, 733 N.W.2d 128, 136 (Minn. 2007). The United States and Minnesota Constitutions protect the right of the people to be free from "unreasonable searches and seizures" of their "persons, papers, and effects" by the government. U.S. Const. amends. IV, XIV; Minn. Const. art. I, § 10; *see Mapp v. Ohio*, 367 U.S. 643, 655–56 (1961) (incorporating the Fourth Amendment and the consequences for violating it into the Due Process Clause of the Fourteenth Amendment).

There is no question here that the police searched McNeilly's home office and her electronic devices. *See State v. Edstrom*, 916 N.W.2d 512, 517 (Minn. 2018) (noting that a search occurs when the government "physically intrudes onto a constitutionally protected area" or "intrudes upon a person's reasonable expectation of privacy"). A search is presumptively unreasonable unless it is conducted under a valid warrant or a specific exception to the warrant requirement applies. *State v. Othoudt*, 482 N.W.2d 218, 221–222 (Minn. 1992). It is undisputed in this case that the searches occurred pursuant to warrants and that no warrant exception applies. Therefore, the search is valid only if the warrants

themselves complied with the requirements of the Fourth Amendment and Article I, Section 10.

A warrant must be supported by probable cause and be sufficiently particular. *State v. Bradford*, 618 N.W.2d 782, 795 (Minn. 2000). McNeilly does not dispute that probable cause existed to support the issuance of the warrants. But she argues that the warrants were not particular enough to satisfy the United States and Minnesota Constitutions. The identical Particularity Clause in each constitution requires that a search warrant "particularly describ[e] the place to be searched, and the person or things to be seized." U.S. Const. amend. IV; Minn. Const. art. I, § 10. "This requirement prohibits law enforcement from engaging in general or exploratory searches," *Bradford*, 618 N.W.2d at 795, and from engaging in "general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). The particularity requirement also "prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927).

We have observed that the description of items in a warrant must only be "as specific as the circumstances and the nature of the activity under investigation permit." *State v. Hannuksela*, 452 N.W.2d 668, 674 (Minn. 1990) (internal quotation marks omitted) (quoting *United States v. Santarelli*, 778 F.2d 609, 614 (11th Cir. 1985)). "[W]hen determining whether a clause in a search warrant is sufficiently particular, the circumstances of the case must be considered, as well as the nature of the crime under investigation and whether a more precise description is possible under the circumstances."

State v. Miller, 666 N.W.2d 703, 713 (Minn. 2003). If a warrant is not sufficiently particular, the general remedy is the suppression of the evidence seized under the warrant. *United States v. Calandra*, 414 U.S. 338, 347 (1974). But under the severance doctrine, if some parts of a warrant are not particular enough and others are particular enough, "insufficient portions of the warrant are stricken and any evidence seized pursuant thereto is suppressed, but the remainder of the warrant is still valid." *Hannuksela*, 452 N.W.2d at 673.

The Supreme Court has recognized that "[t]he Fourth Amendment by its terms requires particularity *in the warrant*, not in the supporting documents." *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (emphasis added). In other words, courts look solely at the face of the warrant in determining whether it was sufficiently particular—i.e., contained sufficient limitations.[6]

B.

McNeilly argues that the office warrant was insufficiently particular because it authorized a general search of her electronic devices without regard to relevance or privilege. The first warrant states that police sought to search McNeilly's home "for the following described property and things": "Documents showing occupancy"; "Digital pictures prior to and during the search"; "Computers such as laptops, desktops, and or

[6] A court may "construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant." *Groh*, 540 U.S. at 557–58; *see also State v. Fawcett*, 884 N.W.2d 380, 387 (Minn. 2016). This exception does not apply here. Neither warrant expressly incorporated the warrant application and no supporting document was attached to either warrant.

towers"; "Electronic devices which could contain or access files held remotely"; "Mobile phone associated with [McNeilly's phone number]"; "Confidential Informant form"; "Any files, invoices, or Documents associated with representation of M.W. and J.S."; and "Retainer agreement for M.W."

The final page of the warrant provides that designated law enforcement officers were authorized "to search the above-described premises, for the described property and thing(s), and to seize and keep said property and thing(s) in custody until dealt with according to law." In other words, the office warrant expressly authorized *seizure* of computers and electronic devices, but it did not explicitly authorize a *search* of them.

The office warrant, in McNeilly's view, authorized not just physical seizure of the electronic devices, but also an unlimited search of those devices. According to McNeilly, this breadth would result in an insufficiently particular warrant because the warrant did not place any restrictions on a potential search of her devices.

The State tacitly agrees that a warrant for seizure of a computer allows a search of the entire contents of the computer. The State insists, however, that the breadth of the warrant did not violate the Particularity Clauses of the U.S. and Minnesota Constitutions because, in his affidavit supporting the warrant, the officer who applied for the office warrant swore under penalty of perjury that he would seek additional warrants to search the electronic devices. According to the State, had he searched the devices without obtaining a second warrant, he would have been guilty of perjury, permanently damaged his reputation, faced civil damages, and risked his entire investigation. Thus, in the State's view, any Fourth Amendment concerns were alleviated.

The State's argument is not well founded. In *Franks v. Delaware*, the United States Supreme Court considered "the alternative sanctions of a perjury prosecution, administrative discipline, contempt, or a civil suit" and concluded that these "are not likely to fill the gap" if the exclusionary rule is unavailable. 438 U.S. 154, 169 (1978). In other words, the State cannot overcome the argument that a warrant is not sufficiently particular by claiming that other constraints deter the police from carrying out the search in an overbroad manner.

McNeilly's argument is also without support. Functionally, her argument is based on three premises: (i) a search—even if reasonable—that is conducted pursuant to an insufficiently particular warrant violates the Fourth Amendment; (ii) the office warrant authorized a search of McNeilly's computer; and (iii) the office warrant placed no restrictions on the search of the computer (and hence, was insufficiently particular). As explained below, her argument fails on the third premise.

The first premise is correct: "a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." *Groh*, 540 U.S. at 559 (internal quotation marks omitted) (quoting *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5 (1984)). In other words, even if the State's search were reasonable, if the warrant was not sufficiently particular, there is still a Fourth Amendment violation and evidence obtained during the search should generally be suppressed.

We have never considered the second premise—whether a search of a computer is authorized when the computer is listed as an item to be seized pursuant to a warrant. We are persuaded, however, by the sound reasoning of other courts that have held that such a

search is authorized by the warrant. The majority of federal courts that have addressed the issue—and the Minnesota Court of Appeals—have held that a search of a computer is authorized when it is listed as an item to be seized pursuant to a warrant. *See United States v. Grimmett*, 439 F.3d 1263, 1269 (10th Cir. 2006) (collecting cases from the First, Sixth, Ninth, and Tenth Circuits that hold that it is unnecessary to obtain a second warrant to search a seized computer); *United States v. Gregoire*, 638 F.3d 962, 967 (8th Cir. 2011) ("A search warrant which specifically authorized the seizure of a computer and a search for financial records clearly contemplates at least a limited search of the computer's contents."); *Gregerson v. Hennepin County*, No. A14-0487, 2014 WL 4957978, at *4 (Minn. App. Oct. 6, 2014); *State v. Taylor*, No. A17-0912, 2018 WL 1462324, at *3 (Minn. App. Mar. 26, 2018). We therefore conclude that the second premise is correct.

But the third premise is incorrect. Although the office warrant listed computers as one of the items to be seized and thus authorized a search of the computer (the second premise), it did not authorize a wholesale or limitless search. Rather, the rule we adopt is that a warrant that authorizes seizure of a computer allows for a search of that computer, but only for the items otherwise listed in the warrant that reasonably may be found on the computer. This approach makes sense because the warrant requirement ensures that there is probable cause to believe that listed items are connected to the crime and that those items will be found on the computer.[7]

[7] As we discuss below, a search limited to the categories in either of the warrants is sufficiently particular to satisfy the Fourth Amendment and Article I, Section 10.

This rule is consistent with a well-reasoned decision of the court of appeals: *Gregerson*, 2014 WL 4957978, at *6. Gregerson had previously sued two companies and their principal shareholder for copyright infringement, malicious prosecution, and similar claims. *Id.* at *1. Later, law enforcement opened a criminal investigation into the companies and principal shareholder based on two suspected crimes unrelated to the litigation with Gregerson. *Id.* Two search warrants were issued. The first warrant was based on probable cause to believe that a building was being used as an unlicensed massage parlor; this warrant authorized a search for massage therapy equipment, advertising materials related to massage therapy, and "computers and peripherals used to place online advertising, produce advertising materials or schedule client appointments." *Id.* The second search warrant was issued based on probable cause to believe that the subject of the warrant had engaged in theft by swindle in the sale of a fake diamond; this warrant authorized a search for financial and other records relating to diamonds and "computers and peripherals used to maintain financial transaction records of the diamond sale or used in the production of fictitious . . . papers." *Id.*

Gregerson sought information on his adversaries, so he demanded—under the Minnesota Government Data Practices Act, Minn. Stat. ch. 13 (2012)—that the police turn over information on the seized computers unrelated to the two criminal investigations. *Id.* at *2. The police refused to provide Gregerson with the information, and the district court rejected Gregerson's claim that the police were required to turn over the information. *Id.* at *2–3.

The court of appeals affirmed. *Id.* at *6. It reasoned that the seizure of the computer under a warrant terminated the owner's expectation of privacy in the information contained on the computer but only to the extent the information otherwise fell within the scope of the warrant. The two warrants did not authorize the police to search for any "other data contained on the hard drives and not identified in the warrant." *Id.* at *4. Because the information Gregerson sought was not related to documents or information relevant to operation of an unlicensed massage parlor or the theft by swindle, any further search by the police of the computers would constitute an unconstitutional search. *Id.* We agree with this reasoning: a warrant to seize a computer also authorizes a limited search of that computer for items included in the warrant that are likely to be found on the computer.

McNeilly—who needs the scope of the office warrant to be construed broadly in order to argue it is not constitutionally particularized—cites two federal decisions in support of her argument that a warrant authorizing the seizure of a computer also authorizes a search of *all* electronic contents: *Gregoire*, 638 F.3d 962 and *United States v. Upham*, 168 F.3d 532 (1st Cir. 1999). In fact, both cases support the rule we adopt today.

In *Gregoire*, the defendant was stealing sporting goods from his employer and selling the goods on eBay. 638 F.3d at 965–66. During the investigation, law enforcement obtained a warrant to seize "financial records" and "all computers on the property." *Id.* at 967. The court concluded that a search of the computer "for records *related to eBay sales* was contemplated and therefore permitted by the warrant." *Id.* at 968 (emphasis added). In other words, the court concluded that a search warrant that "specifically authorized the

seizure of a computer" as well as items likely to be found on that computer "clearly contemplates . . . a limited search of the computer's contents." *Gregoire*, 638 F.3d at 967.

Likewise, in *Upham*, the court noted that the warrant authorized seizure of computers as well as "[a]ny and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct." 168 F.3d at 534. The court noted that "the seizure and subsequent off-premises search of the computer . . . was about the narrowest definable search and seizure reasonably likely to obtain the images." *Id.* at 535. In other words, a seized computer may be searched for other items listed in the warrant, provided those items might reasonably be found within the computer's digital contents. *See* Fed. R. Crim. P. 41(e)(2)(B) (stating that a warrant that authorizes "seizure of electronic storage media" also, "[u]nless otherwise specified . . . authorizes a later review of the media or information *consistent with the warrant*." (emphasis added)).

Applying these principles here, the office warrant did not authorize an unlimited search of McNeilly's devices. Rather, the scope of the search of the computer authorized by the office warrant was limited to the items identified in the warrant that could be found on a computer: confidential informant forms; files, invoices, or documents associated with McNeilly's representation of M.W. and J.S; and retainer agreements for M.W.[8] McNeilly does not otherwise claim the items listed on the office warrant are insufficiently particular. Accordingly, we conclude that the office warrant was sufficiently particular.

[8] Moreover, the scope of the ultimate search of McNeilly's electronic devices was limited to the items specified in the second warrant.

C.

McNeilly also charges that the device warrant was insufficiently particular. We start with the language of the warrant. It authorized a search of McNeilly's devices for "Files related to communications, calendar events, invoices, retainer agreements, and documents pertaining to MW and JS"; "Calendar events, communications or docs showing contact with [the Minnetonka detective]"; "Confidential Informant form"; and "Any files or notes associated with representation of M.W. and J.S." In addition to certain named members of law enforcement, the warrant authorized the following persons to search the electronic devices: "Dakota County Electronics Crimes Unit [personnel], peace officers of the State of Minnesota, and any other authorized person."

McNeilly offers five reasons why the device warrant was insufficiently particular. According to McNeilly, the warrant was constitutionally invalid because it (i) failed to specify procedures to protect privileged attorney-client communications and work-product materials; (ii) failed to limit the search to a time period after the search of M.W.'s home on May 1, 2018; (iii) failed to limit the search to documents related to the crime (i.e., McNeilly's theft by swindle); (iv) authorized seizure of contacts with the Minnetonka detective even if those contacts did not pertain to M.W. and J.S.; and (v) authorized seizure of all documents pertaining to a confidential informant form without restrictions on date or client. We address each of these reasons in turn.

i.

McNeilly argues that the device warrant was insufficiently particular because it failed to list procedures to safeguard privileged attorney-client communications and

work-product materials. McNeilly asks us to adopt a rule that every search warrant must expressly state that the police are required to take steps to screen out communications protected by the attorney-client privilege as well as attorney work product—even when the warrant involves a search of the law office of a lawyer who is suspected of a crime. We decline to adopt such a rule.

As we discuss in greater detail below, we are cognizant of the special circumstances surrounding the search of an attorney's office, particularly where, as here, the attorney represents criminal defendants. *See O'Connor v. Johnson*, 287 N.W.2d 400, 404 (Minn. 1979) (noting that "[a] criminal defendant's constitutional right to counsel . . . must . . . be weighed in determining the reasonableness of a search warrant" and that "we must take care to protect . . . the rights of all clients of the attorney whose office is being searched"). But McNeilly did not cite a single case invalidating a search as insufficiently particular because the warrant itself did not specify privilege-protection measures. Moreover, the particularity requirement is not the optimal tool to protect privileged attorney-client communications and work-product materials in a law office search. Requiring rigid privilege protocols within a warrant creates challenges because members of law enforcement (and the magistrate issuing the warrant) do not yet know what will be found.[9]

---

[9] Broad privilege protections in a warrant—such as specifying that each category of documents sought must be 'non-privileged' or stating that officers must 'take reasonable precautions to safeguard privileged materials'—face similar obstacles. Law enforcement will then be using their judgment—again, without advance knowledge of what, exactly, they will find—in trying to comply with the warrant. This quickly becomes a constitutional reasonableness analysis. To be clear, we are not saying that judges should never include limitations in warrants to protect the privilege; such limitations may be appropriate and

Cf. In re Search Warrant Issued June 13, 2019 ("*Baltimore Law Firm*"), 942 F.3d 159, 178 (4th Cir. 2019) (noting that authorizing a filter protocol 5 days before the search warrant was executed "undermined the judge's ability to exercise discretion with respect to the Filter Team and its Protocol" and that "the judge should have deferred the decision concerning the proposed Filter Team and its Protocol pending the execution and return of the search warrant").

For those seeking to safeguard privileged documents in a search, it is more appropriate to ask whether the search, as it was actually conducted, was constitutionally reasonable. This totality of the circumstances analysis allows for more flexibility and nuance. In sum, we conclude that the Particularity Clause does not require that every warrant list specific privilege-screening procedures for law-office searches. Such a rule would not only be unprecedented, but also ineffective.

McNeilly argues that even if the Particularity Clause does not mandate privilege safeguards in a warrant, the warrant here nonetheless undermined the attorney-client privilege and work-product doctrine by allowing members of the investigation and prosecution team to access materials protected by those doctrines. Specifically, the warrant authorized "Dakota County Electronics Crimes Unit [personnel], . . . peace officers of the State of Minnesota, and any other authorized person" to conduct the search of McNeilly's electronic devices. According to McNeilly, even if the examiner were the only person to actually conduct the search, her search was pursuant to an invalid warrant and thus violates

---

even beneficial in certain cases. We are rather deciding that such limitations are not constitutionally required under the Particularity Clause.

the Fourth Amendment. *Groh*, 540 U.S. at 559–60 (holding that even if a search is reasonable as executed, this does not cure a facially invalid warrant).

The problem with this argument is that it challenges neither the location of the search, nor the items to be seized, but rather the persons conducting the search. This challenge goes beyond the text of the Particularity Clause, which provides that "no Warrants shall issue, but upon probable cause . . . and particularly describing the *place to be searched, and the persons or things to be seized*." U.S. Const. amend. IV (emphasis added). McNeilly does not point us to a single decision that invalidated a warrant under the Particularity Clause based on the persons authorized to conduct the search.

ii.

McNeilly next contends that the search of her devices should have been limited temporally to communications on or after May 1, 2018—the date of the police search of M.W.'s home.[10] When evaluating particularity of a warrant, "the circumstances of the case must be considered, as well as . . . whether a more precise description is possible under the circumstances." *Miller*, 666 N.W.2d at 713.

Here, it was not possible to specify a more precise time frame in the warrant. Communications before May 1, 2018, could be relevant evidence because the parties disputed the reason that M.W. paid McNeilly $15,000. That dispute required an

[10] When the examiner conducted the search, she only reviewed documents dated on or after May 1, 2018. That fact is not constitutionally relevant. Assuming—contrary to our holding today—that a warrant allowing the police to search for materials before May 1 was insufficiently particular, the fact that the police self-limited the search to the constitutionally permissible timeframe would not cure a facially invalid warrant. *Groh*, 540 U.S. at 559–60.

investigation into the full scope of McNeilly's representation of M.W., including monies paid and/or owed for any legal work McNeilly had provided on M.W.'s landlord-tenant dispute, his drug case, or any other case. That is why the application for the device warrant included "retainer agreements, casefiles, and documents pertaining to M.W. and J.S." The warrant application specifically stated that "[t]hese files, if located, could be used to confirm or contradict M.W.'s assertion that McNeilly has not provided legal services on his behalf for the [monies] which he provided to her for the retainer and the 'donation' to the police fund."

iii.

McNeilly argues that the particularity requirement demands that warrants specify the crime to which the documents must relate. In support of this contention, McNeilly cites *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995).

Kow centered around an FBI raid of a video cassette distribution company that was suspected of defrauding a related company and the Internal Revenue Service. *Id.* at 425. The court observed:

> [T]he warrant apparently sought to describe every document on the premises and direct that everything be seized. The government emphasizes that the warrant outlined fourteen separate categories of business records. However, the warrant contained no limitations on which documents within each category could be seized or suggested how they related to specific criminal activity.

Id. at 427.

Contrary to McNeilly's assertion, *Kow* did not set out a rule that a warrant must specify the crime being investigated. The *Kow* court applied the correct standard:

"[g]eneric classifications in a warrant are acceptable only when a more precise description is not possible." *Id.* (citation omitted) (internal quotation marks omitted); *see also Miller*, 666 N.W.2d at 713 (reasoning that when evaluating particularity of a warrant, courts must consider "whether a more precise description is possible under the circumstances").

In *Kow*, the government did not provide *any* limits on which documents could be seized. The court concluded that a more precise description was possible. The court suggested that the "[m]ost obvious[]" limitation would be to "specif[y] the suspected criminal conduct." *Kow*, 58 F.3d at 427. But it suggested numerous other ways the government could have made the warrant more particular, including limiting the scope of the seizure "to a time frame within which the suspected criminal activity took place" or limiting the documents sought to those that include the suspect company's "tax identification number . . . account number at the Bank of Trade, or the names of the foreign companies allegedly receiving the proceeds." *Id.*

In this case, it was not immediately apparent during the investigation what the crime was—initial reports suggested bribery, but ultimately investigators determined that the crime was theft by swindle. Even if the warrant had specified either bribery or theft by swindle as the suspected crime under investigation, it is not clear that specifying either or both as suspected crimes would significantly circumscribe the warrant. The device warrant specifically described files for two clients, one of whom was swindled and the other who witnessed key events in the swindle case. (This is analogous to the *Kow* court's suggestion that the search be limited to documents associated with certain companies or banks central to the crime). M.W.'s housing court file was relevant to the crime because the State was

investigating what legal services, if any, had been provided in exchange for the monies paid. Likewise for communications with the Minnetonka detective—specifying that the crime in question was alleged bribery would authorize seizure of the same documents pertaining to the detective. And at the time, the police did not know if McNeilly would continue to claim that the bribery scheme was real. Put differently, although it is true that the device warrant could have specified the crime being investigated, it would not have altered the scope of the search authorized by the warrant.

iv.

McNeilly argues that the device warrant was insufficiently particular because it authorized seizure of all contacts between McNeilly and the Minnetonka detective, including those that pertained to clients other than M.W. and J.S. We disagree. The search of all communications with the detective was justified because this investigation originated from allegations that he was accepting a bribe. And the actual communications between McNeilly and the Minnetonka detective were still relevant to showing that McNeilly had swindled M.W. by falsely claiming that law enforcement was extorting her client. And in seeking evidence that McNeilly and the Minnetonka detective were—or were not—engaged in a bribery scheme, police were within their rights to seek communications between those two, even if those communications did not pertain to M.W. or J.S. After all, a bribery scheme between a criminal defense attorney and a detective may suggest an ongoing relationship that extends beyond a single client.

Further, even assuming the provision about contacts with the Minnetonka detective were insufficiently particular, the outcome would not change. Under our precedent, we

would exclude any evidence seized under the 'contacts with [the Minnetonka detective]' provision. *See Hannuksela*, 452 N.W.2d at 673. No evidence pertaining to communications with the Minnetonka detective was ever used or introduced, so there is nothing that would require exclusion.

v.

Finally, McNeilly argues that the device warrant was insufficiently particular because it authorized seizure of all documents pertaining to a confidential informant form, regardless of the client to whom that form related or the date it was prepared.

"[W]hen determining whether a clause in a search warrant is sufficiently particular, the circumstances of the case must be considered, as well as the nature of the crime under investigation and whether a more precise description is possible under the circumstances." *Miller*, 666 N.W.2d at 713. The warrant application provided that "M.W. stated that McNeilly showed him an example of the CI form." Further, M.W. refused to sign a confidential informant form when McNeilly made the request. Thus, police had information that McNeilly had shown M.W. a copy of a confidential informant form, but not whether it had a date or person's name on it. The confidential informant forms ultimately seized and presented at trial did not have names or dates included. One form was from the Texas Alcoholic Beverage Commission and the other was a forgery—based on the Texas form—that purported to be from the Southwest Hennepin Drug Task Force. Given these facts, it is not apparent that a more precise description of the confidential informant form in question was possible under the circumstances.

* * *

In summary, we hold that both warrants in this case were sufficiently particular under the United States and Minnesota Constitutions.

II.

Separate from her particularity claims, McNeilly contends that the search warrants were executed in an unreasonable manner under the Fourth Amendment and Article I, Section 10, because the police did not take adequate steps to identify and exclude from the search privileged communications and lawyer work product.

A.

A government agent conducting a search can violate the Fourth Amendment by performing the search without proper judicial authorization, *Groh*, 540 U.S. at 562–63, by seizing evidence beyond that which is authorized in the warrant, *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388, 394 n.7 (1971), or by executing the search in an unreasonable manner, *Dalia v. United States*, 441 U.S. 238, 258 (1979). McNeilly's argument that the State failed to implement reasonable privilege safeguards falls into the third category: unreasonable execution of a search.

"When officers obtain a warrant to search an individual's home, they also receive certain limited rights to occupy and control the property; however, the Fourth Amendment binds the officers such that the right to search a home concomitantly obliges the officers to do so in a reasonable manner." *San Jose Charter of Hells Angels Motorcycle Club v. City of San Jose*, 402 F.3d 962, 971 (9th Cir. 2005) (internal quotation marks omitted) (quoting *Lawmaster v. Ward*, 125 F.3d 1341, 1350 (10th Cir. 1997)). "[W]hen executing a search

warrant, an officer is limited to conduct that is reasonably necessary to effectuate the warrant's purpose." *Lawmaster*, 125 F.3d at 1349; *see Ginter v. Stallcup*, 869 F.2d 384, 388 (8th Cir. 1989). In *Bell v. Wolfish*, the United States Supreme Court explained:

> The test of reasonableness under the Fourth Amendment is not capable of precise definition or mechanical application. In each case it requires a balancing of the need for the particular search against the invasion of personal rights that the search entails. Courts must consider the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted.

441 U.S. 520, 559 (1979). McNeilly argues that the scope of the intrusion is considerable when police search an attorney's files because there is a very high probability that they will contain privileged communications or attorney work product. Thus, a search of a lawyer's files has serious potential to undermine the values underlying the attorney-client privilege and the work-product doctrine as well as constitutional protections of criminal defendants set forth in the Fifth and Sixth Amendments to the United States Constitution and corresponding protections set forth in the Minnesota Constitution.

McNeilly notes that the attorney-client privilege provides space for open and complete communication between a lawyer and client. An attorney "can only effectively fulfill [her] roles as counselor, intermediary, and advocate if the client, assured of confidentiality, is wholly free to completely and candidly disclose all the facts, favorable or unfavorable." *Kahl v. Minn. Wood Specialty, Inc.*, 277 N.W.2d 395, 398 (Minn. 1979). The work-product doctrine—which protects from disclosure "an attorney's mental impressions, trial strategy, and legal theories in preparing a case for trial," *Dennie v. Metro. Med. Ctr.*, 387 N.W.2d 401, 406 (Minn. 1986)—is likewise essential for effectively serving

her clients. Accordingly, McNeilly argues, a search of an attorney's office, even when the attorney is suspected of a crime, presents a substantial intrusion into private and sensitive matters, and the manner of the search must be carefully scrutinized. As discussed above, although the police in this case took steps to make sure the documents that were turned over to the prosecution team were relevant, they did not consider whether the documents they were reviewing were privileged or protected by the work-product doctrine. As McNeilly observes, that is troubling.

McNeilly relies on our decision in *O'Connor*, which involved the search of a law office when the lawyer was *not* the target of the investigation. 287 N.W.2d at 404. In that case—which has been our law for nearly half a century—we recognized the sanctity of the attorney-client privilege and work-product doctrine when police search a law office. *Id.* We said that "[i]n protecting these rights and privileges we must take care to protect . . . the rights of all clients of the attorney whose office is being searched." *Id.* In other words, a search of an attorney's office implicates concerns about the privacy interests of clients who entrust their attorney with sensitive privileged information in order to receive full and effective representation.

Indeed, we recognized in *O'Connor* that a search of a law office—especially the office of a criminal defense attorney—gives the attorney-client privilege a constitutional dimension. We observed:

> A criminal defendant's constitutional right to counsel, guaranteed by Article I, section 6 of the Minnesota Constitution and the Sixth Amendment of the United States Constitution, must also be weighed in determining the reasonableness of a search warrant under Article I, section 10 of the

> Minnesota Constitution and the Fourth Amendment of the United States Constitution.

Id. at 404. We also observed that mere disclosure to police could be incredibly damaging: "[o]nce [privileged] information is revealed . . . the information cannot be erased from the minds of the police." *Id.* at 405; *see also Kaur v. Maryland*, 141 S. Ct. 5, 6–7 (2020) (statement Sotomayor, J., respecting denial of certiorari) (noting some of the "many insidious ways" privileged information can be used against a criminal defendant). Based on these concerns, we adopted rules to regulate the search of a lawyer's office when the lawyer was not the subject of the police investigation. The protections we established were rooted in part in our power "to afford . . . greater protection [under Article I, Section 10, of the Minnesota Constitution] than the safeguards guaranteed in the Federal Constitution." *O'Connor*, 287 N.W.2d at 405.

McNeilly also relies on *State v. Flowers*, 986 N.W.2d 686 (Minn. 2023). In *Flowers*, we reaffirmed the constitutional dimension of the attorney-client privilege: "although the attorney-client privilege is . . . a statutory right codified under Minn. Stat. § 595.02, subd. 1(b) (2022) . . . it is relevant to a Sixth Amendment right-to-counsel analysis." *Id.* at 694.

According to McNeilly, federal courts have diligently scrutinized the procedures used to protect privileged material and work product because of the tremendous risks involved in the search of a law office. *See, e.g.*, *United States v. Regan*, 281 F. Supp. 2d 795, 802 (E.D. Va. 2002). "[S]earches and seizures of items from law offices are not unreasonable, *per se*, if measures are taken to protect certain privileges that might attach

to documents contained therein." *Id.*; *see also Klitzman, Klitzman & Gallagher v. Krut*, 744 F.2d 955, 959 (3d Cir. 1984) (noting that where an attorney is the target of a criminal investigation, a search of a law office is not "*per se* unreasonable" and that "the correct approach to this issue . . . is not to immunize law offices from searches, but to scrutinize carefully . . . the nature and scope of the search, and any resulting seizure"). McNeilly also cites to a number of other federal courts that have scrutinized the procedures used to safeguard privileged and work-product materials during searches of law offices, but with one exception we have identified, those courts have not expressly determined that a search without such protections is constitutionally unreasonable.[11] *See, e.g.*, *United States v.*

---

[11] The exception is *United States v. Renzi*, 722 F. Supp. 2d 1100 (D. Ariz. 2010). In that case, a federal court in Arizona specifically found that failure to follow protocols to prevent disclosure of privileged documents to the government rendered a search—in that case, a wiretap—unreasonable. *Id.* at 1127. Federal investigators obtained a warrant to wiretap a congressman; the warrant detailed procedures to protect privileged information, and those procedures were not followed. *Id.* at 1105–10. The court concluded that "[t]he Government's conduct, in its totality, warrants a more significant sanction than just suppressing the privileged evidence. The Court suppresses the wiretap." *Id.* at 1111.

Renzi is not decisive of the issue presented here. First, it is not binding on us. Second, unlike *Renzi*, in this case the district court had not specified, in advance, procedures to protect privileged materials that the police then ignored. Third, unlike *Renzi*, this prosecution stems from an investigation of an *attorney*, not the attorney's client; a difference we find significant as discussed below. Finally, the privileged communications in *Renzi* were shared with the prosecution team as well as with co-defendants. The record here is not so clear. McNeilly correctly points out that no privilege review was conducted. But the record does not reveal whether, despite that serious oversight, privileged communications or work-product materials were reviewed by the examiner or turned over to the prosecution team. The record does not reveal that any of the documents in the files of McNeilly that were searched were in fact privileged communications or work-product material and McNeilly does not identify any that were so used. This lack of record is one reason that we hesitate to reach the constitutional issue in this case.

We also take note of a case from the Third Circuit, *Klitzman*, 744 F.2d at 960, where the court found that a search of a law office was overbroad because it authorized a search

Stewart, No. 02 CR. 395 JGK, 2002 WL 1300059, at *3 (S.D.N.Y. June 11, 2002); *Baltimore Law Firm*, 942 F.3d at 176; *United States v. Ritchey*, 605 F. Supp. 3d 891, 902 (S.D. Miss. 2022).

We emphasize that unlike our prior decision in *O'Connor* and many of the federal decisions, in this case, the lawyer—not the lawyer's client—is the target of the police investigation. This distinction is significant because the attorney-client privilege belongs to the client and not the attorney. It is the client that has the protected privacy interest, not the lawyer. *In re Houge*, 764 N.W.2d 328, 340 (Minn. 2009); *State v. Tall*, 45 N.W 449, 450 (Minn. 1890). We know that the privilege belongs to the client because "[a] *client* can waive his or her attorney-client privilege either by explicit consent or by implication." *State v. Walen*, 563 N.W.2d 742, 752 (Minn. 1997) (emphasis added); *see* Minn. Stat. § 595.02, subd. 1(b) (2022) ("An attorney cannot, without the consent of the attorney's client, be examined as to any communication made by the client to the attorney or the attorney's advice given thereon in the course of professional duty . . . ."). Once the client has waived the privilege, the lawyer can no longer use the privilege as a shield against discovery or disclosure at trial. *See Walen*, 563 N.W.2d at 752 (noting that implicit waiver occurs when a client alleges that her attorney breached a duty to the client and concluding

---

of "all client files, open or closed" as well as "the seizure of all of the firm's financial records, file lists, and appointment books." It discussed the potential for privilege violations at length, but did not clarify whether that would, on its own, justify its finding that the search was overbroad. *Id.* at 961. Moreover, the court did not reach the ultimate issue of whether the Fourth Amendment was violated, but rather affirmed the issuance of a preliminary injunction. *Id.* at 962.

that the client waived the privilege by bringing an ineffective-assistance-of-counsel claim).[12]

In other words, the prohibition against intruding into the attorney-client privilege exists to protect the client, not to protect the attorney. Consequently, there is a legitimate question as to whether a lawyer in her individual capacity[13] has a sufficient expectation of

---

[12] The State argues that M.W. waived the privilege as to all his communications with McNeilly when he reported McNeilly's scheme to the police. We are not convinced, however, that M.W.'s discussions with the police about McNeilly's acts on November 5, 2018, constitute a wholesale waiver of every attorney-client communication that M.W. may have had with McNeilly. The scope of an implicit waiver of the attorney-client privilege is limited to "communications relevant to that issue." *Walen*, 563 N.W.2d at 752; *see also Fort James Corp. v. Solo Cup Co.*, 412 F.3d 1340, 1349 (Fed. Cir. 2005) ("The widely applied standard for determining the scope of a waiver of attorney-client privilege is that the waiver applies to all other communications relating to the same subject matter."). M.W's communications with law enforcement waived the privilege as to the events surrounding McNeilly's swindle. We are not convinced, and will not assume, that M.W. intended to waive the privilege as to all communications with McNeilly regarding the underlying drug offense or the earlier housing court matter. Indeed, it seems unlikely that such a broad waiver was intended or effectuated, especially when one considers that M.W.'s communications with law enforcement were through Paule, the attorney who succeeded McNeilly as M.W.'s counsel for the drug charge.

In addition, the record in this matter is insufficiently developed to allow us to know the full extent of the communications between McNeilly and M.W. McNeilly did not identify any attorney-client communications with M.W. that were introduced as evidence. On the other hand, the police failed to consider whether privileged communications were included in the files they searched and did not make any record of the documents that were reviewed by the examiner and turned over to the Burnsville Police Department. Consequently, it is impossible for us to determine if McNeilly's files included communications with M.W. on issues that were not waived when he made his statements to the police about the events of November 5. Based on our resolution of this case, we need not definitively resolve the issue of whether M.W. waived the attorney-client privilege with regard to all his communications with McNeilly.

[13] We acknowledge that, as McNeilly argues, attorneys have a professional obligation to assert the attorney-client privilege on behalf of clients. Minn. R. Prof. Conduct 1.6; *O'Connor*, 287 N.W.2d at 403 (noting that an attorney is required "to preserve the

privacy in privileged or work-product materials to allow her to challenge a search as constitutionally unreasonable. *See State v. deLottinville*, 890 N.W.2d 116, 119 (Minn. 2017) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978), for the principle that "standing to bring a Fourth Amendment claim hinges on whether [the defendant] has 'a legitimate expectation of privacy in the invaded place' ").

A somewhat more complicated question is whether an attorney who is under investigation can claim that a search is unreasonable based on inadequate protections for attorney work product. The work-product doctrine protects from disclosure an attorney's opinions, conclusions, mental impressions, trial strategy, and legal theories in materials prepared in anticipation of litigation. *See Dennie*, 387 N.W.2d at 406; Minn. R. Crim. P. 9.02, subd. 3; Minn. R. Civ. P. 26.02(d). Underlying the doctrine is the understanding that nondisclosure of an attorney's work product is essential to mounting an effective defense and disclosure of work product can reveal the same sensitive information conveyed in attorney-client communications. *Hickman v. Taylor*, 329 U.S. 495, 511 (1947) (noting

---

confidences and secrets of his clients"). As a result, attorneys facing a warranted police search of their law office are put in the difficult position of having an obligation to assert the privilege without necessarily having any constitutional standing to challenge the warrant on the ground that the search may invade privileged communications with their clients. *See State v. deLottinville*, 890 N.W.2d 116, 119 (Minn. 2017) ("Fourth Amendment rights are 'personal' and 'may not be vicariously asserted.' " (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969))). This tension is particularly pronounced when clients whose rights are implicated in the search have nothing to do with the matter the police are investigating. Recognition of this tension is one of the reasons that we exercise our supervisory powers, discussed below, to adopt procedural safeguards that apply when the police search the office of a lawyer who is suspected of a crime, to protect disclosure of privileged attorney-client communications and work-product materials. Those restrictions are described fully in Part III below.

that absent the protections of the work-product doctrine, "[i]nefficiency, unfairness and sharp practices would inevitably develop . . . . And the interests of the clients and the cause of justice would be poorly served").

A lawyer may retain some greater interest in work product consisting of mental impressions, conclusions, opinions, or legal theories related to a case than the lawyer has under the attorney-client privilege. We have never expressly addressed the issue of whether a lawyer has an independent interest in work-product materials.[14] But even if we assume without deciding that a lawyer retains such an independent interest unrelated to

---

[14] Some other courts have held that, unlike the attorney-client privilege, "the work[-]product privilege belongs to both the client and the attorney, either one of whom may assert it. Thus, a waiver by the client of the work[-]product privilege will not deprive the attorney of his own work[-]product privilege, and vice versa." *In re Grand Jury Proc.*, 43 F.3d 966, 972 (5th Cir. 1994); *see also In re Special Sept. 1978 Grand Jury*, 640 F.2d 49, 63 (7th Cir. 1980); *First Wis. Mortg. Tr. v. First Wis. Corp.*, 86 F.R.D. 160, 163 (E.D. Wis. 1980); *see generally* Fred C. Zacharias, *Who Owns Work Product?*, 2006 U. Ill. L. Rev. 127, 134–36 (2006) (discussing different federal rulings regarding waiver of work-product doctrine). On the other hand, section 90 of the Restatement (Third) of the Law Governing Lawyers adopts the contrary position that "work-product immunity may be invoked by or for a person on whose behalf the work product was prepared" and "[w]hen lawyer and client have conflicting wishes or interests with respect to work-product material, the lawyer must follow instruction of the client." Restatement (Third) of the L. Governing Laws. § 90 and comment c (Am. L. Inst. 2000).

Note that, under Minnesota Rules of Professional Conduct 1.16(d), upon termination of representation, a lawyer has a responsibility to return materials in the client's file to the client, with two exceptions. In litigation matters, a lawyer need not return "pleadings, discovery, motion papers, memoranda and correspondence which have been drafted, but not served or filed if the client has not paid the lawyer's fee for drafting or creating the documents." Minnesota Rule of Professional Conduct 1.16(e)(2)(i). Similarly, in transactional representations, an attorney need not return "drafted but unexecuted estate plans, title opinions, articles of incorporation, contracts, partnership agreements, or any other unexecuted document which does not otherwise have legal effect, where the client has not paid the lawyer's fee for drafting the document(s)." Minnesota Rule of Professional Conduct 1.16(e)(3).

protecting the client's interest in some work-product materials, that interest is limited to a general interest in the proper functioning of the legal profession, *In re Special Sept. 1978 Grand Jury*, 640 F.2d 49, 62 (7th Cir. 1980) (discussing the majority and concurrence in *Hickman*, 329 U.S. 495), and a more specific interest in avoiding unnecessary and unfair disclosure of the lawyer's economic or competitive interest in her unique approach to legal questions. *See, e.g.*, Fred C. Zacharias, *Who Owns Work Product?*, 2006 U. Ill. L. Rev. at 127–28 and 146. The broader interest in the proper functioning of the legal profession is not personal to a lawyer under criminal investigation. And an economic interest or competitive advantage interest on its own is not a basis for preventing *law enforcement* from obtaining documents as part of a warranted search supported by probable cause of a person suspected of a crime. Consequently, in the specific context of this case—a search of a lawyer's office where the lawyer is the subject of a criminal investigation—the lawyer cannot hide behind the work-product doctrine if her client has waived the benefit of that doctrine.

We must emphasize, however, that the fact that a lawyer may not have an independent interest under the attorney-client privilege does not mean that broader constitutional concerns that we identified in *O'Connor* fall away. When the police investigating a lawyer for a crime demonstrate probable cause and obtain a warrant to search the lawyer's office, a tension exists. On the one hand, police searches of law offices involve a considerable intrusion into private and sensitive privileged communications and work-product materials; clients have privacy interests in those materials. Further, as discussed above, privilege and work-product protections have important constitutional

implications for a lawyer's clients—implications that bear on whether a search satisfies the Fourth Amendment requirement that the police execute search warrants in a reasonable manner. On the other hand, the reason we protect privileged communications and a primary reason we limit disclosure of work-product materials is to shield the client and *not* the lawyer as an individual.

McNeilly asserts that this tension should be resolved by a holding that a search of a law office where the lawyer is the subject of the investigation without any (let alone sufficient) safeguards for privileged communications and work-product materials is a violation of the Fourth Amendment and Article I, Section 10. We decline to accept that invitation in this case. Even if we assumed that, because the police did not review the seized materials for privileged communication or work product materials, the warrants to search McNeilly's office and devices were executed in an unreasonable manner in violation of the Fourth Amendment or Article I, Section 10, McNeilly is not entitled to a new trial. Because the jury's verdict was surely unattributable to the district court's decision not to suppress evidence for unreasonable execution of the searches, the alleged constitutional error was harmless beyond a reasonable doubt. We explain why below.

B.

When determining whether a defendant was prejudiced by the admission of evidence that should have been excluded, we apply one of two different harmless-error tests. When an error does not implicate a constitutional right, we ask whether "there is a reasonable possibility that the wrongfully admitted evidence significantly affected the verdict." *State v. Cram*, 718 N.W.2d 898, 904 n.1 (Minn. 2006). But when the error

implicates a constitutional right, we employ a heightened standard and ask whether the error was harmless beyond a reasonable doubt. *State v. Davis*, 820 N.W.2d 525, 533 (Minn. 2012). "An error is harmless beyond a reasonable doubt if the jury's verdict was surely unattributable to the error." *State v. Sanders*, 775 N.W.2d 883, 887 (Minn. 2009).

McNeilly was charged with theft by swindle under Minnesota Statutes section 609.52, subdivision 2(a)(4). To prevail, the State had to prove that M.W. gave up possession of his property (the $15,000) due to a swindle; that McNeilly intended to obtain for herself or someone else possession of the property; and that McNeilly's act was a swindle. *State v. Pratt*, 813 N.W.2d 868, 873 (Minn. 2012). "The essence of a swindle is the defrauding of another of his property by deliberate artifice." *State v. Olkon*, 299 N.W.2d 89, 106 (Minn. 1980); *see* Minn. Stat. § 609.52, subd. 2(a)(4) (defining theft by swindle as obtaining property or services from another person "by artifice, trick, device, or any other means"). In other words, the State had to prove that McNeilly intentionally tricked M.W. into paying her $15,000—which she intended to keep—based on her fraudulent story that the $15,000 would be used as a down payment on a bribe to the police union.

The State presented overwhelming evidence that McNeilly engaged in a swindle. M.W. and J.S. both testified in detail about an elaborate plot by McNeilly. They explained how she had urgently summoned them on November 5, 2018, and told them that she had met with the Minnetonka detective and prosecutors who were building a massive federal case against M.W. They testified that McNeilly claimed that a federal bug had been planted in M.W.'s house by a renter and subsequently removed by the Minnetonka detective. They

described McNeilly's proposal: M.W. faced 15–20 years in federal prison, but he could avoid charges if he paid $35,000 to the police union and acted as a confidential informant. When M.W. said he did not want to be an informant, McNeilly offered him a second option: pay $50,000 to the police union and no service as a confidential informant would be necessary. M.W. and J.S. testified that M.W. agreed to the $50,000 option and indicated that he could pay $15,000 that day. McNeilly went to M.W.'s garage—ostensibly to make a phone call—and emerged 5 or 10 minutes later claiming that the detective had agreed to the deal.

That same day, at McNeilly's insistence, M.W. provided McNeilly with a cashier's check for $15,000. There is no dispute that M.W. paid her $15,000. M.W. testified to that fact and his testimony was supported by bank records (obtained directly from the bank) which showed a $15,000 deposit on the same day.

Other evidence that did not come from the search of McNeilly's law office showed McNeilly confirming M.W.'s story. M.W. provided law enforcement with a series of text and email exchanges between him and McNeilly. For instance, M.W. sent McNeilly an email stating "I am unable to move forward with the plan discussed at my home" and asking her to return the $15,000. In response, McNeilly texted M.W. as follows: "Yes, I got your email. It was paid as directed. So how can I get a refund? This is a serious issue." Notably, McNeilly did not contest that the $15,000 was for a "plan discussed" on November 5 and did not assert that the money was for past services. Instead, McNeilly asked how *she* could get a refund—indicating that she had paid the funds to a different party—which is consistent with M.W.'s testimony that McNeilly told him she would send the money to the

Minnetonka detective in exchange for dismissal of M.W.'s drug charges. The conclusion that a refund was unavailable because "[i]t was paid as directed" also strongly suggests that McNeilly was, at the time, still trying to maintain the ruse of buying off law enforcement.

The defense theory at trial was that the $15,000 was paid for legal services McNeilly had rendered to M.W. prior to November 5, 2018 (the date of payment). McNeilly's argument to the jury was that M.W. made up the bribery scheme to avoid having to pay for legal services rendered.[15] The only evidence she introduced in support of this theory was an invoice which was dated November 5, 2018. The "for" line states "Invoice from 5/15/18-11/4/18." The invoice lists various tasks purportedly performed, including "Hearing Prep" and "Court Appearance(s)" without listing dates when work was performed. The total comes to $16,075 and at the bottom is handwritten "Paid $15,000 11/5/18."

McNeilly's theory, however, does not stand up to scrutiny. In determining whether an error was harmless beyond a reasonable doubt, "overwhelming evidence of guilt" is a relevant and often important factor, although certainly not a dispositive factor. *See State v. Al-Naseer*, 690 N.W.2d 744, 748 (Minn. 2005). First and critical under the unique facts of this case, the theory that the $15,000 was paid for legal services rendered is inconsistent with McNeilly's own words in her text message to M.W. on November 8, 2018, which

---

[15] Even if M.W. had owed McNeilly the money, it could still be theft by swindle if she obtained the funds by artifice, trick, device, or similar means. *See State v. Lone*, 361 N.W.2d 854, 860 (Minn. 1985) (holding that it is not a defense to theft by swindle to say that the victim received something of value); *State v. Andrade*, No. A06-797, 2007 WL 1598849, at *5 (Minn. App. June 5, 2007) ("[A] claim of right is irrelevant to the crime of theft by swindle.").

confirms M.W.'s story by stating, "Yes, I got your email. It was paid as directed. So how can I get a refund? This is a serious issue." In the text, McNeilly did not refute that she and M.W. had a plan for using the $15,000, that the $15,000 "was paid as directed," and that she could not get a refund from the person to whom she had paid the money. McNeilly did not assert that the money was for past services—which would have been the obvious response if that was the reason M.W. paid her $15,000.

Indeed, the record does not disclose how M.W. could accrue over $16,000 in legal fees—purportedly for more than 50 hours of legal work—for a criminal matter that authorities had not yet charged.[16] Moreover, the $15,000 in "legal fees" was in addition to the $20,000 fee that M.W. had already paid on the uncharged matter.[17]

---

[16] M.W.'s housing court case was summarily resolved after two hearings and M.W. had paid $2,000 in advance on that matter. J.S.'s drug charge was quickly resolved with a guilty plea, and a flat fee of $2,500 had been paid to McNeilly for that representation.

[17] The retainer agreement purports to be an 'availability retainer,' in which a client pays not for legal services, but for the availability of the attorney (i.e., an option for future representation). *See* Minn. R. Prof. Conduct 1.5(b)(2). But the retainer agreement also lists services McNeilly would provide in exchange for the fee paid:

> 2. SCOPE OF SERVICES: Client hires Lawyers to provide legal services in the following matters: Availability retainer fee only for possible drug trafficking case-per client conversation. If charges develop at a later date, new retainer must be signed. Will research warrant on home and arrange bail if needed. Will take steps to get defense ready for possible case.

This retainer is not an availability retainer because it details legal services to be provided in exchange for the fee. *See* Minn. R. Prof. Conduct 1.5(b)(2) ("A lawyer may charge a fee to ensure the lawyer's availability to the client . . . on a specified matter in addition to and apart from any compensation for legal services performed."). In other words, the "research" and other "steps to get defense ready for possible case" theoretically performed by McNeilly would be covered by the $20,000 payment and could not be separately charged at $300 per hour as the invoice purports to do.

In addition, the State provided bank records that showed M.W. paid McNeilly $15,000 on November 5. M.W. and J.S. testified to McNeilly's proposed bribery scheme. And, perhaps most importantly, none of the evidence discussed so far was obtained in the searches of McNeilly's office and electronic devices.

The State did introduce some of the evidence it obtained in the search to support its case. In particular, the State introduced the Texas Bureau of Alcohol Confidential Informant Form that had been downloaded to McNeilly's computer on November 5, 2018, and the identical form, with the heading changed to "Southwest Hennepin Drug Task Force" that was created on McNeilly's computer. The State also entered into evidence the actual (very different) confidential informant form used by the Southwest Hennepin Drug Task Force (a document not in McNeilly's files).

This evidence supports the conclusion that McNeilly had lied about the possibility of acting as a confidential informant. We observe that the State did discuss the confidential informant agreements in closing, but overall, after review of the record, we conclude that the State did not give the forms significant focus at the trial and the forms were not highly persuasive in the context of the trial. *See State v. Caulfield*, 722 N.W.2d 304, 317 (Minn. 2006) (discussing other non-exclusive factors that overcome strong evidence of guilt if they support the conclusion that the error was harmful). In particular, the evidence demonstrating that McNeilly fabricated the story about a federal drug investigation and a bribery scheme to convince M.W. to pay her $15,000 included McNeilly's own contemporaneous words maintaining the ruse that she was using the $15,000 to pay the police union. Accordingly, we conclude that the jury's decision to find McNeilly guilty of

theft by swindle was surely unattributable to the State's use of the two confidential informant forms.[18]

III.

As discussed above, in *O'Connor* we recognized that in the search of a law office—especially the office of a criminal defense attorney—the attorney-client privilege takes on a constitutional dimension for the lawyer's clients. It is true that in *O'Connor*, the lawyer was not the target of the police investigation. Our concern about the constitutional implications for a lawyer's clients of allowing the police to gain access to privileged attorney-client communications and work-product materials, however, is not diminished simply because the target of an investigation is the lawyer whose office is searched rather than one of the lawyer's clients.

In *O'Connor*, we adopted a special prophylactic rule for police searches of law offices where the lawyer is not the target of the investigation to protect the constitutional rights of the lawyer's clients. We held that the police searching the office of an attorney who is not the subject of a criminal investigation must proceed by subpoena duces tecum rather than by search warrant. 287 N.W.2d at 405. That process allows an attorney—on behalf of her clients—"to assert applicable privileges by a motion to quash." *Id.* The process also provides the benefit of judicial review of privilege claims. We required these procedures—even though we recognized that the procedures may "limit[] the ability of the

[18] The State also used invoices it had obtained in the searches of McNeilly's office and computer to discredit the November 5, 2018, invoice introduced by McNeilly. As explained above, this document was discredited in several other ways that did not require resort to evidence found in the searches.

police to obtain information in the early stages of an investigation"—because of the vital interest in protecting privileged materials from disclosure. *Id.*

We also observed in *O'Connor* that the risk of an attorney frustrating a search for documents implicating a client in a crime is limited. We reasoned that lawyers have a professional obligation to turn over all responsive documents (again subject to a motion to quash) and there was no indication that the lawyer in *O'Connor* would attempt to destroy the documents before disclosure. *Id.* We agree with the State that the solution we adopted in *O'Connor*—a requirement that the police proceed by subpoena duces tecum rather than search warrant—is a poor fit if the lawyer is the subject of the police investigation. When the lawyer is the target of a search, among other complications, the risk that the lawyer may attempt to hide or destroy evidence in response to a subpoena rises. Thus, we conclude that the subpoena requirement adopted in *O'Connor* is not appropriate when a search targets an attorney.

Accordingly, we turn to the question of the procedures necessary to safeguard the client's interests—as recognized in *O'Connor*—when the *lawyer* is the target of the investigation. "It is our duty to supervise the criminal justice system and ensure the fair administration of justice." *State v. Windish*, 590 N.W.2d 311, 319 (Minn. 1999). "[T]he thread that binds our court's interests-of-justice jurisprudence is . . . quite simple: our court must, at times, act as a backstop—the court of last resort—to protect the human, political, and property rights guaranteed by the constitution." *State v. Thompson*, 994 N.W.2d 554, 560 (Minn. 2023) (citation omitted) (internal quotation marks omitted).

As part of that duty, we have the inherent authority to regulate and supervise the rules that govern the admission of evidence in the lower courts. *State v. Obeta*, 796 N.W.2d 282, 287 (Minn. 2011); *State v. Hill*, 871 N.W.2d 900, 909 (Minn. 2015). We have exercised that authority to adopt rules to ensure the fair administration of justice. For instance, we have adopted rules that place limitations on admission of evidence where law enforcement has not followed certain procedures. *See, e.g.*, *State v. Scales*, 518 N.W.2d 587, 592 (Minn. 1994) (requiring police to record in-custody interrogations); *State v. Lefthand*, 488 N.W.2d 799, 801–02 (Minn. 1992) (holding that in-custody interrogation of a formally accused person who is represented by counsel must not proceed prior to notification of counsel or the presence of counsel).[19]

We conclude that the need to safeguard the client's constitutionally protected interests—as recognized in *O'Connor*—is substantial. In determining the procedures necessary to protect those interests when the *lawyer* is the target of the investigation, our decision in *Scales*, 518 N.W.2d at 592, is instructive.

In *Scales*, the defendant disputed law enforcement accounts of his custodial interrogation. *Id.* at 590. He argued that he had the right under the Minnesota Constitution

[19] We have also used our supervisory powers to require the State to take affirmative actions and provide procedural safeguards—essentially prophylactic rules to safeguard constitutional rights. *See State ex rel. Doe v. Madonna*, 295 N.W.2d 356, 365 n.17 (Minn. 1980) (requiring a preliminary probable cause hearing); *State v. Borst*, 154 N.W.2d 888, 894 (Minn. 1967) (requiring an attorney for a criminal defendant charged with a misdemeanor); *Hepfel v. Bashaw*, 279 N.W.2d 342, 348 (Minn. 1979) (requiring an attorney for indigent defendants in paternity adjudications "where the complainant is represented by the county attorney"); *Scales*, 518 N.W.2d at 592 (requiring electronic recording of all custodial interrogations).

to have his custodial interrogation recorded. *Id.* at 590–91. We declined to decide the issue under the Minnesota Constitution, but also recognized that the constitutional interests in avoiding self-incrimination and coerced confessions would be served by a prophylactic rule that both "creat[es] an accurate record of a defendant's interrogation for trial and appeal" and "discourag[es] unfair and psychologically coercive police tactics." *State v. Castillo-Alvarez*, 836 N.W.2d 527, 536 (Minn. 2013) (quotation omitted) (explaining the reasons for the rule established in *Scales*). Thus, we exercised our supervisory powers and required recording of custodial interrogations, holding that failure to do so would result in suppression of statements from the interrogation. *Scales*, 518 N.W.2d at 592.

We have recognized that the threat to the attorney-client privilege and work-product doctrine is not limited to *use* of the materials by an adversary but can also result from the *disclosure* of privileged communications and work-product materials. *See O'Connor*, 287 N.W.2d at 405 ("Once [privileged] information is revealed to the police . . . the information cannot be erased from the minds of the police."). Indeed, our efforts to protect privileged communications and work-product materials are focused on preventing *disclosure* of the communications and materials and on ensuring review of any disputes over the privileged or protected nature of communications and work-product materials by a neutral third party before disclosure.

For instance, in the context of civil litigation, privileged materials are not just shielded from admission by the Minnesota Rules of Evidence—they may be withheld from disclosure to opposing parties under Minnesota Rule of Civil Procedure 26.02(f)(1). The withholding party must provide the requesting party with a privilege log identifying the

documents not produced. Minn. R. Civ. P. 26.02(f)(1). Further, if privileged communications or work-product material are inadvertently disclosed in litigation, the party who received it (upon being notified the disclosing party is claiming the documents are privileged or work product) "must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim [of privilege] is resolved." Minn. R. Civ. P. 26.02(f)(2); *see* Minn. R. Evid. 502. In either case, the claim of privilege or work-product protection is reviewable by a court. *See* Minn. R. Civ. P. 26.02 (Advisory Committee Comment—2007 Amendment). In addition, a party may seek information from a third party under a subpoena. In that case, a similar process is followed. Minn. R. Civ. P. 45.04(b).

The subpoena duces tecum requirement for searches of the office of a lawyer when the lawyer is not the target of an investigation includes a similar focus on preventing disclosure of privileged communications and work-product materials and allowing a neutral magistrate to review disputes over the privileged or work-product status of materials before the State gains access to them. *O'Connor*, 287 N.W.2d at 405. We conclude that the rule for searches of the office of a lawyer who is the subject of the investigation should have a similar focus on preventing disclosure and allowing neutral magistrate review.

Accordingly, and pursuant to our supervisory powers, in the context of searches of law offices where the lawyer is the subject of the search, we direct as follows:

All documents obtained from a search of a law office are presumed to be privileged.[20] This principle follows from the premise that "a matter committed to a professional legal adviser is prima facie so committed for the sake of the legal advice . . . and is therefore within the privilege unless it clearly appears to be lacking in aspects requiring legal advice." *Kobluk v. Univ. of Minn.*, 574 N.W.2d 436, 442 (Minn. 1998); *see also In re Polaris, Inc.*, 967 N.W.2d 397, 414 (Minn. 2021) (Anderson, J., dissenting) ("We therefore presume that a communication regarding a matter committed to an attorney is privileged in its entirety . . . ."); *United States v. Pedersen*, No. 3:12-CR-00431-HA, 2014 WL 3871197, at *31 (D. Or. Aug. 6, 2014) ("The only entity that is entitled to make a determination that a private communication between an attorney and her client is *not* privileged is the court." (emphasis added)). Not only are documents in an attorney's file likely to be privileged communications, but a file is also likely to contain work product prepared by the attorney on the client's behalf. Accordingly, when the police search an attorney's law office, the initial burden to show the documents are not privileged rests with the State.

The State can satisfy its initial burden to demonstrate that documents are neither privileged nor work product by establishing (without the prosecution team reviewing the documents) (i) that the documents fail to meet the elements of those protections; (ii) that the attorney-client privilege has been waived by the client or that the work-product

[20] Note that documents that are not obtained in the search—such as a client file that is provided by the client—are not presumed privileged, so the court need not make a final privilege determination; those documents may be provided to and used by the prosecution team immediately.

protection has been waived pursuant to existing law; or (iii) that an exception to the privilege (e.g., crime-fraud) applies.

The presumption of privilege is contrary to the general rule that "the party resisting disclosure bears the burden of presenting facts to establish the privilege's existence." *Kobluk*, 574 N.W.2d at 440. But the general rule makes little sense in a context in which a vast number of documents are likely to be subject to the attorney-client privilege and work-product doctrine and the documents are searched and seized under circumstances that do not permit a timely and effective opportunity to assert privilege.

As a corollary to the presumption of privilege, review of files should be limited as much as practicable during the search process. For example, if a warrant authorizes seizure of a particular client's file and the fact that it is a particular client's file is clear without opening it, there is no need to open the physical file (or the relevant electronic file) during the search and before the privilege review by a neutral magistrate or designee or by a taint team as discussed below.

Second, the initial screening for privileged communications and work-product materials included among the seized documents must be undertaken by an entity other than the investigation and prosecution team. Before information is provided to the prosecution team, the court should verify that the attorney-defendant has notified clients impacted by the potential disclosure to the prosecution. If the attorney-defendant does not notify clients in a timely manner, the court may take appropriate action to protect the client files in a

manner that does not unnecessarily delay the criminal investigation or prosecution.[21] The investigation and prosecution team should not have access to the contents until the file has been screened and a neutral magistrate has had the opportunity to review disputes over the privileged or work-product status of materials. *See O'Connor*, 287 N.W.2d at 405.

The more "traditional" approach to reviewing sensitive documents is to submit those documents "under seal for in camera review by a neutral and detached magistrate or by court-appointed special masters." *United States v. Neill*, 952 F. Supp. 834, 841 & n.13 (D.D.C. 1997). Other courts have allowed review by an independent taint team. *See In re Ingram*, 915 F. Supp. 2d 761, 764 (E.D. La. 2012) (collecting cases and noting that several courts "have approved the use of government filter teams").

If law enforcement uses a taint team to screen documents, the district court must, with input from the taint team, the attorney-defendant, and her clients who express interest, review and approve the process the taint team will use to ensure that sufficient safeguards are in place to protect from disclosure privileged communications and work product materials. The process must at a minimum ensure that:

---

[21] We reinforce our statement from *K.M.* that following the seizure of documents from an attorney's office, a district court should order the immediate return of copies of the attorney's files. 940 N.W.2d at 172. We emphasized that return of client files is crucial so an attorney can "fulfill her professional responsibilities. This includes not just advising her clients in ongoing matters, but also notifying clients that their open and closed files have been seized by law enforcement so that those clients can take timely steps to protect their rights." *Id.* (observing that an attorney's professional responsibilities include "notifying clients that their open and closed files have been seized by law enforcement"); Minn. R. Prof. Conduct 1.4(a), 1.7.

(i) The taint team is disinterested, does not include any members of the investigation or prosecution team, and is walled off from the investigation and prosecution team;[22]

(ii) The State strictly limits access to any material it holds to necessary personnel and controls are implemented so that the State knows which personnel have accessed the material;

(iii) Privilege determinations are made by attorneys;[23] and

(iv) There is a meaningful opportunity for disputed privilege and work-product determinations to be adjudicated by the court (or another neutral magistrate or special master appointed by the court).[24] *In re Polaris, Inc.*, 967 N.W.2d

---

[22] *Cf. United States v. Stewart*, No. 02 CR. 395 JGK, 2002 WL 1300059, at *7 (S.D.N.Y. June 11, 2002) (noting that when reviewing privileged documents obtained in a search, the procedure adopted should "not only be fair but also appear to be fair"); *In re Grand Jury Subpoenas*, 454 F.3d 511, 523 (6th Cir. 2006) (observing that if the filter team has too many connections with the prosecution team, it compounds the appearance that "the government's fox is left in charge of the [law firm's] henhouse"); *Baltimore Law Firm*, 942 F.3d at 182 (rejecting filter team procedures where the filter team "includes prosecutors employed in the same judicial district where Law Firm clients 'are being investigated by, or are being prosecuted by' " the same prosecutor's office).

[23] *Cf. In re Search of Elec. Commc'ns in the Acct. of chakafattah@gmail.com at Internet Serv. Provider Google, Inc.*, 802 F.3d 516, 530 (3d Cir. 2015) (reprimanding prosecutors where they "include[d] a non-attorney federal agent at the first level of review, followed by review by independent attorney federal agents" because "first level of privilege review should be conducted by an independent . . . attorney"); *see also Baltimore Law Firm*, 942 F.3d at 177 (remanding for greater privilege protections where "the [privilege protocol] authorized paralegals and IRS and DEA agents to designate seized documents as nonprivileged").

[24] Law enforcement does not need a court's permission to review documents if it is satisfied that it has obtained clear, adequate waiver of both the attorney-client privilege and

at 410 ("When facts are presented upon which the claimed privilege rests, it then becomes necessary for *the court* to determine whether the privilege exists much the same as in the determination of other fact issues." (emphasis added) (internal quotation marks omitted) (quoting *Brown*, 62 N.W.2d at 701)).[25]

Third, the State should take precautions regarding data access and retention for evidence obtained in the search of a law office. For instance, Amicus Tony Webster rightly points out that law enforcement data breaches do happen. *See* Tony Webster, *Personal information of Minnesota law enforcement, critical infrastructure personnel published online after massive hack*, Minnesota Reformer (July 10, 2020), https://minnesotareformer.com/2020/07/10/personal-information-of-minnesota-law-enforcement-critical-infrastructure-personnel-published-online-after-massive-hack/ (last visited Apr. 5, 2024) [opinion attachment]. The record does not reveal any information about security practices for McNeilly's data. We do not know if the data was segregated

---

the work-product doctrine. Law enforcement should be cautious, however, because this court has not had opportunity to rule upon the sufficiency of a waiver of work-product doctrine, especially where a client has waived the doctrine and her attorney has not. If the court later determines that waiver was not sufficient, the government risks exclusion of all fruits from the search.

[25] *Cf. United States v. Vepuri*, 585 F. Supp. 3d 760, 764 (E.D. Pa. 2021) (stating that "[t]he authority to determine issues of privilege belongs to the courts and the courts alone" because to allow the State to make final privilege determinations would "undermine[] the separation of powers and vitiate[] significant interests of the defendant"); *Baltimore Law Firm*, 942 F.3d at 176 (stating that "a court is not entitled to delegate its judicial power and related functions to the executive branch, especially when the executive branch is an interested party in the pending dispute").

from other cases or if law enforcement would know whether there was an intrusion upon the information or the identity of the intruder. In the event of a data breach (i.e., the unauthorized acquisition or release of personally identifying information), the State must inform the attorney-defendant.

If these procedures are not followed, the district court, on motion made by the attorney-defendant or one of her clients, may exclude from evidence any documents or objects obtained in or derived from the search, including non-privileged documents. In exercising this remedial power, the district court retains discretion to deny the exclusion of evidence that is not protected by the attorney-client privilege or work-product doctrine if the court finds after considering the totality of the circumstances that the State's violation of the procedures we announce today was not substantial. *See Scales*, 518 N.W.2d at 592 (stating that "suppression will be required of any statements obtained in violation of the recording requirement if the violation is deemed 'substantial' "). But as in *Scales*, "[i]f the court finds a violation not to be substantial, it shall set forth its reason for such finding." *Id.*

The rule and remedy we announce today will apply prospectively to searches conducted after the date of the filing of this opinion. We do not apply these new rules to this case because the remedy—suppression of evidence obtained in the search—would not change the outcome. *See supra* at section II.B. We do not need to decide today whether the harmless error or constitutional harmless-error test applies to these new rules because, as explained above in section II.B, the outcome would not change even under the higher, constitutional standard.

CONCLUSION

For the foregoing reasons, we affirm the decision of the court of appeals.

Affirmed.

PROCACCINI, J., not having been a member of this court at the time of submission, took no part in the consideration or decision of this case.

C O N C U R R E N C E

ANDERSON, Justice (concurring).

I concur. I write separately to note the undecided constitutionality of taint teams in Minnesota. *See State v. Flowers*, 986 N.W.2d 686, 691 n.5 (Minn. 2023) (expressing no opinion on the constitutionality of taint teams generally because the issue was not raised by the parties). I would reiterate here our observation in *Flowers*: that federal courts have expressed reservations about leaving "the government's fox . . . in charge of the appellants' henhouse." *Id.* (quoting *In re Grand Jury Subpoenas*, 454 F.3d 511, 523 (6th Cir. 2006)) (internal quotation marks omitted). In 2019, for example, the United States Court of Appeals for the Fourth Circuit concluded that taint teams violated the separation of powers because "a court simply cannot delegate its responsibility to decide privilege issues to another government branch." *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 177 (4th Cir. 2019).

Although the constitutionality of taint teams is an important issue, it is neither argued nor decided here. But given the scrutiny of this practice from other courts, our supervisory directions as to the outer bounds of permissible taint team procedure should not be construed as a tacit endorsement of the constitutionality of taint teams generally. *See In re Search of Elec. Commc'ns in the Acct. of chakafattah@gmail.com at Internet Serv. Provider Google, Inc.*, 802 F.3d 516, 530 n.53 (3d Cir. 2015) (establishing certain restrictions on the use of taint teams despite the case presenting "no occasion to consider the appropriate limits, if any" on the use of taint teams generally).

THISSEN, Justice (concurring).

I join in the concurrence of Justice Anderson.

GOVERNMENT & POLITICS

Personal information of Minnesota law enforcement, critical infrastructure personnel published online after massive hack

BY: **TONY WEBSTER** - JULY 10, 2020 3:37 PM

The offices of the Minnesota Bureau of Criminal Apprehension, one of the agencies involved in the breach. Photo by Tony Webster/Minnesota Reformer.

A trove of Minnesota law enforcement data was published online after hackers broke into the servers of a vendor of the Minnesota Bureau of Criminal Apprehension and Hennepin County Sheriff's Office.

The sensitive information includes details about key Minnesota security and intelligence personnel at every level of government.

Also released were personally identifying contact information for security personnel for critical infrastructure sites in Minnesota like nuclear power plants, chemical processing facilities, rail networks, pipelines, hospitals and campuses of major employers and schools.

Information on over 9,000 government and industry personnel dating back over 15 years were divulged in a breach of data from ICEFISHX, an intelligence sharing and emergency alert website, which is part of the Minnesota Fusion Center, the intelligence wing of the Minnesota Bureau of Criminal Apprehension.

The breach of data of the Hennepin County Sheriff's Office included the names and contact information of approximately 1,500 first responders, corporate security personnel and key security staff at sports stadiums, all who participated in their "Shield" information sharing program.

Names, titles, ranks, employers, addresses, mobile phone numbers, pager numbers, email addresses, IP addresses and more were included in the databases, and some entries noted the importance of some of the members and the sensitivity of their facilities.

"Monitoring of the electrical grids for Minnesota and surrounding states," said one entry in the Minnesota Fusion Center database. "[O]ne of the largest user[s] and packag[er] of Chlorine (UN1017) in the Upper Midwest," read another. "Our [redacted by the Minnesota Reformer] plant makes bullets and our [redacted by the Minnesota Reformer] site tests new explosives and equipment," said another line in the file. In many cases, the Minnesota Fusion Center had categorized individuals in the databases into groups like "Agricultural Chemicals" and "Nuclear Materials and Waste."

The *Reformer* verified that several of the cell phone numbers included in the data breach were accurate, including an assistant chief at Minneapolis FBI; the chief operating officer of the Federal Reserve Bank of Minneapolis; a military antiterrorism officer; an intelligence research specialist at the DEA; high-level security staff at a Minnesota nuclear power plant; and employees who operate the corporate command centers and cyber threat response groups at two large publicly-traded companies.

The stolen data was contained in "BlueLeaks," which is being called the largest leak of U.S. law enforcement data in history, and was

published online in mid-June by Distributed Denial of Secrets, a team of transparency activists who say they have no political leaning.

Spokespersons for the Minnesota Bureau of Criminal Apprehension, Minnesota Homeland Security Emergency Management, and Hennepin County Sheriff's Office were reached by phone and email for comment, but did not provide a response by the time of publication.

Immediately after publication, Jill Oliveira, spokeswoman for the BCA, provided a statement, which said the data was illegally obtained.

"The Minnesota Fusion Center has received from the FBI a copy of the portion of the stolen documents related to Minnesota Fusion Center activities. The Fusion Center is in the process of evaluating the data for not public information on individuals and will notify individuals as needed," said Oliveira.

The hacked data included over 20,000 files, such as intelligence briefings, software code, suspicious activity alerts, COVID-19 situation reports, violent offender advisories, as well as internal information such as codewords to use when reporting suspected terrorist activity. But some of the most sensitive data might be information on first responders and those keeping Minnesota's critical infrastructure safe.

Aside from passwords, the information in the leak was not encrypted, suggesting major shortcomings in the information security practices of both Minnesota state government and its largest jurisdiction, Hennepin County. The *Reformer* presented a list of questions to the Minnesota Department of Public Safety about whether they are investigating the breach, whether any of the individuals named in the breach had been informed, and what steps have been taken in the nearly month since the information was published online. The agency did not respond.

Because some of the data stolen in the hack was not public under law, the hacking may qualify as a data breach, requiring the

government agencies involved to provide notice to individuals in the database. Several people whose data was leaked told the *Reformer* they had not been informed of the breach, despite the agencies' legal obligation to do so.

One federal law enforcement officer who works undercover said they had no knowledge that their name, agency affiliation and cell phone number had been published on the Internet.

The stolen data included identifying information on personnel who work in security and intelligence at local police departments and sheriff's offices, ambulance companies and hospitals, emergency management teams throughout the Twin Cities metro area, Metro Transit, the Federal Reserve Bank, courthouse security, chemical threat and pandemic teams at the Minnesota Department of Health, conservation officers, military force protection and intelligence teams and federal officers at the ATF, FBI, Secret Service, ICE and the U.S. Marshals.

The hacked data had been housed at Netsential, a vendor of both the Minnesota Bureau of Criminal Apprehension and Hennepin County Sheriff's Office.

"Netsential can confirm its web servers were recently compromised," read a statement posted on the company's website. "We have enhanced our systems and will continue to work with law enforcement to mitigate future threats."

Mark Lanterman, chief technology officer at Computer Forensic Services and a former member of a Secret Service Electronic Crimes Task Force, said the breach highlights the risks of outsourcing: "This shows that you're only as secure as your vendors," he said. Audits to ensure vendor compliance with security requirements are common in the private sector, but not government, he said.

"Law enforcement has decided to outsource some of their needs to vendors that perhaps they should have been auditing," Lanterman said. "There's no such thing as perfect security, and without someone conducting an audit, they're still at risk."

He said the typical advice of changing passwords after a data breach still applies, but that this type of data breach presents a broader safety issue.

"My guess is half of law enforcement read about [BlueLeaks] as a headline, didn't bother to read the rest of the article, and is totally oblivious to what data is out there," said Lanterman. "I really think law enforcement needs to reevaluate how they're managing this."

Asked what law enforcement agencies should do now that the data has spread across the internet, Lanterman said: "Pray."

TONY WEBSTER

Tony Webster is a journalist and photographer. He won the Minnesota Society of Professional Journalists 2017 Peter S. Popovich Award for his freedom-of-information advocacy.

MORE FROM AUTHOR

RELATED NEWS

Minnesota Republicans introduce legislation inspired by the…

BY **CHRISTOPHER INGRAHAM**

April 5, 2024

Legislature considering up-front sales tax break for…

BY **MICHELLE GRIFFITH**

April 4, 2024

The Minnesota Reformer is an independent, nonprofit news organization dedicated to keeping Minnesotans informed and unearthing stories other outlets can't or won't tell. We're in the halls of government tracking what elected officials are up to — and monitoring the powerful forces trying to influence them. But we're also on the streets, at the bars and parks, on farms and in warehouses, telling you stories of the people being affected by the actions of government and big business. And we're free. No ads. No paywall.

We're part of States Newsroom, the nation's largest state-focused nonprofit news organization.

DEIJ Policy | Ethics Policy | Privacy Policy

v1.6.0

STATES NEWSROOM

FAIR. FEARLESS. FREE.