IN THE COURT OF APPEALS OF THE STATE OF ALASKA

ERIN A. POHLAND, Appellant, v. STATE OF ALASKA, Appellee.	Court of Appeals No. A-12443 Trial Court No. 3AN-12-1066 CR O P I N I O N No. 2624 — November 23, 2018

Appeal from the District Court, Third Judicial District, Anchorage, Jo-Ann Chung, Judge.

Appearances: Cynthia L. Strout, Anchorage, for the Appellant. Michal Stryszak, Assistant Attorney General, Office of Criminal Appeals, Anchorage, and Jahna Lindemuth, Attorney General, Juneau, for the Appellee.

Before: Mannheimer, Chief Judge, and Allard and Wollenberg, Judges.

Judge MANNHEIMER.

Erin A. Pohland, a former assistant attorney general, appeals her conviction for official misconduct, AS 11.56.850(a). The State alleged that Pohland used her position as legal advisor to the Alaska Labor Relations Agency to benefit her personal friend, Skye McRoberts.

Much of the evidence against Pohland was based on information obtained during a search of her personal computer. This computer was seized when the state troopers executed a search warrant for Skye McRoberts's house — where Pohland was renting an apartment. The troopers were looking for evidence of *McRoberts's* potential business and financial crimes, but they seized Pohland's computer under the theory that McRoberts might have hidden evidence of her crimes in any computer or electronic storage device located within the house — even Pohland's personal laptop, which was found in Pohland's apartment.

Pohland contends that the search of her computer violated her rights under the Fourth Amendment and under the corresponding provision of the Alaska Constitution (Article I, Section 14). We agree with Pohland that the search of her computer was unlawful. Even when the police have a warrant to search a house, a personal computer must be treated differently from other objects or containers in the house. As the United States Supreme Court explained in *Riley v. California*,[1] a police search of this kind of personal digital device "[will] typically expose to the government far more than the most exhaustive search of a [person's] house", because the device "not only contains in digital form many sensitive records previously found in the home", but also "a broad array of private information never found in a home in any form".[2]

As we explain in this opinion, the troopers did not have probable cause to believe that Pohland's personal laptop computer contained evidence of her landlord's financial and business crimes. Moreover, rather than confining their search to documents and spreadsheets (*i.e.*, computer files that were more likely to contain evidence of financial and business crimes), the troopers obtained much of the evidence against

---

[1] 573 U.S. __, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014).

[2] *Riley*, 573 U.S. at __, 134 S.Ct. at 2491.

Pohland by combing through thousands of Pohland's personal text messages. (Pohland was using her laptop computer as a backup device for the data stored on her smart phone.)

For these reasons, we reverse Pohland's conviction.

Underlying facts

Pohland and Skye McRoberts were close friends, and Pohland lived in an apartment (*i.e.*, a suite of rooms) within McRoberts's house.

Pohland was also an assistant attorney general who advised the Alaska Labor Relations Agency — the agency within the executive branch that dealt with labor union matters.

Pohland's friend McRoberts worked as a union organizer for the Alaska State Employees Association. The State Employees Association was engaged in an effort to unionize the employees of the University of Alaska. In connection with this effort, McRoberts submitted employee "interest" cards to the Labor Relations Agency — cards purporting to express the interest of various University employees in becoming members of the union. (Under Alaska law, at least 30 percent of a proposed bargaining unit must express interest in becoming unionized.[3])

The Labor Relations Agency came to suspect that a number of these interest cards might have been forged, so the Agency contacted Pohland for advice. Based on the advice that Pohland gave to the Labor Relations Agency, Pohland was charged with official misconduct.

---

[3] *See* 08 AAC 97.060(c).

Specifically, the State alleged that Pohland failed to tell the Agency that she was close friends with McRoberts, that she lived in an apartment within McRoberts's home, that she had regularly discussed the unionization effort with McRoberts, and that she had assisted McRoberts in this effort. The State further alleged that Pohland's advice to the Labor Relations Agency was designed to shield her friend McRoberts from any official investigation into the possibility that McRoberts had forged, or had colluded in forging, the employee interest cards.

The seizure and search of Pohland's computer, and the litigation of the suppression motion in the trial court

In March 2011, the Alaska State Troopers obtained a warrant to search McRoberts's house for evidence that she and her husband, Donavahn McRoberts, had committed forgery and falsification of business records relating to the forged interest cards. More specifically, the search warrant authorized the troopers to search the house for various kinds of documents "related to the business and finances" of McRoberts and her husband, as well as documents related to the solicitation of potential union members from the University of Alaska.

When the troopers applied for this search warrant, they knew that Pohland was good friends with McRoberts, they knew that the Labor Relations Agency had sought advice from Pohland regarding the forged interest cards, and they knew that there were reasons to question the competence of Pohland's advice to the Labor Relations Agency.

In particular, the search warrant affidavit recited that Pohland's advice to the Labor Relations Agency "did not follow the guidelines for forged Interest Cards laid out in a National Labor Relations Manual". The search warrant affidavit also asserted

that Pohland "failed to advise [the Agency] to contact law enforcement to investigate the matter", and that Pohland failed to tell the Labor Relations Agency that she was good friends with McRoberts and that McRoberts was her landlord.

However, both the troopers and the prosecutor assigned to the case later conceded that, when the troopers applied for the warrant, they did not have probable cause to believe that Pohland was complicit in McRoberts's crimes.

The search warrant issued by the district court contained a provision authorizing the troopers to seize and search any computer or electronic storage media "capable of concealing documents related to the business and finances associated with Donavahn McRoberts or Skye McRoberts."

During the troopers' ensuing search of McRoberts's house, the troopers identified Pohland's separate apartment within the house. This area of the house did not have separate egress to the street, but it was a suite of rooms comprising a bedroom, a separate kitchen, a separate bathroom, and a clothes washer and dryer.

While the troopers were searching Pohland's apartment, they seized a laptop computer. At the time, the troopers conducting the search presumed that the laptop belonged to Pohland. A subsequent examination of the laptop's hard drive confirmed this assumption. The laptop contained numerous documents belonging to Pohland, as well as thousands of text messages between Pohland and various people (backup copies of texts from Pohland's mobile phone).

Many of these text messages were exchanged between Pohland and McRoberts, and some of these text messages appeared to discuss the campaign to unionize the university workers. These text messages became part of the State's case against Pohland when she was later charged with official misconduct for the advice that she gave to the Labor Relations Agency.

After Pohland was charged, her attorney asked the district court to suppress the evidence obtained from the search of Pohland's laptop.

Pohland's attorney argued that Pohland's apartment was a separate living space, and that the warrant authorizing a search of McRoberts's house did not encompass Pohland's apartment. In the alternative, the defense attorney argued that the troopers did not have probable cause to believe that Pohland's personal laptop contained information relevant to the crimes that the troopers were investigating (*i.e.*, the crimes allegedly committed by McRoberts and her husband).

Following an evidentiary hearing, the district court denied Pohland's suppression motion.

In its ruling, the district court acknowledged that, "generally, if a structure is divided into more than one occupancy unit, probable cause must exist for each unit [which is] to be searched." The district court acknowledged that Pohland "had her own living space" within McRoberts's house, and that Pohland paid rent for this apartment. The court also found that the entrance door into Pohland's apartment was lockable — even though that door was not locked when the troopers executed the search warrant.

However, the district court concluded that Pohland's apartment within McRoberts's house was not so sequestered as to constitute a separate occupancy unit for Fourth Amendment purposes. The district court reached this conclusion because Pohland's apartment did not have its own separate egress to the street, because McRoberts and Pohland were close friends (*i.e.*, their relationship was not simply landlord and tenant), and because the court found that McRoberts continued to have "general access" to Pohland's apartment "as the landlord and owner of the house".

The district court further concluded that, even though the troopers presumed from the outset that the laptop seized from Pohland's apartment belonged to Pohland, and not McRoberts, the troopers nevertheless had probable cause to believe that

Pohland's laptop contained evidence of McRoberts's crimes. The district court pointed out that the entry door to Pohland's apartment was inside McRoberts's house, and that "there was no evidence that ... McRoberts was blocked from access to Pohland's apartment." The court also again pointed out that Pohland and McRoberts were not simply tenant and landlord; instead, they were close friends.

The district court acknowledged (based on the investigating trooper's testimony, and based on the prosecutor's express concession) that when the troopers applied for the search warrant, they did not have probable cause to believe that Pohland herself had committed any crime. Nevertheless, the district court concluded that the troopers had probable cause to believe that McRoberts might have concealed evidence of *her own* crimes within Pohland's living area — including hiding this evidence on the hard drive of Pohland's laptop computer.

The court therefore ruled that the search warrant authorized the troopers to seize and search Pohland's laptop.

A preliminary note on the issue of whether the troopers could lawfully enter Pohland's apartment to search for evidence of McRoberts's crimes

As we noted in the preceding section of this opinion, the State concedes that when the troopers applied for the search warrant, they did not have probable cause to believe that Pohland was complicit in McRoberts's crimes, or that Pohland was knowingly concealing evidence of McRoberts's crimes. Pohland argues that the troopers therefore failed to establish probable cause to search her personal apartment within McRoberts's house.

As explained in Professor LaFave's treatise on search and seizure law, "a search warrant for an apartment house or hotel or other multiple-occupancy building will

usually be held invalid if it fails to describe the particular subunit to be searched". Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* (5th ed. 2012), § 4.5(b), Vol. 2, pp. 731-32. To prevent the police from searching the subunits indiscriminately without probable cause, a search warrant for a multiple-occupancy building must normally be supported by a showing of probable cause as to each unit to be searched. See the cases cited in *LaFave*, § 4.5(b), n. 64, Vol. 2, pp. 732-33.

This multiple-occupancy rule does not apply in situations where a single residence is occupied by several people or families who share the common living quarters, even though they each have a separate bedroom. *Id.*, § 4.5(b), Vol. 2, p. 741. But in Pohland's case, as we have explained, her apartment was a suite that contained a separate kitchen, a separate bathroom, and clothes washing appliances.

Indeed, the search warrant application implicitly acknowledged that Pohland's apartment was a separate subunit within McRoberts's house. The application explained that McRoberts was Pohland's landlord, and the application expressly sought permission to search "any part of the residence ... that may be occupied or considered to be in the control of Ms. Pohland."

The proposed justification for searching Pohland's apartment was that McRoberts was Pohland's landlord, and that Pohland and McRoberts were close friends — thus suggesting that McRoberts might have gained access to Pohland's apartment and hidden evidence of her own crimes there.

In its decision, the district court ruled that the search of Pohland's apartment was lawful because the evidence presented at the later suppression hearing showed that McRoberts may have had physical access to Pohland's portion of the house. In particular, the district court relied on evidence that, even though the main door to Pohland's apartment *could be* locked, it *was not* locked when the troopers entered the

house to execute the search warrant. From this, the district court concluded that "there was no evidence that Skye McRoberts was blocked from access to Pohland's apartment."

But it was not Pohland's burden to show that McRoberts was affirmatively *blocked from access* to her apartment. Rather, it was the State's burden to prove that McRoberts *did, in fact, have access* to Pohland's apartment. Moreover, this showing had to be made in the search warrant application itself, not from after-acquired information. And the critical question was not whether McRoberts was capable of physically entering Pohland's apartment. The issue here was whether the search warrant application offered reason to believe that McRoberts had control over Pohland's apartment to such a degree that she would use that apartment to hide evidence of her own wrongdoing.

Despite our questions about the district court's ruling on this issue, we conclude that we need not resolve these questions. As we explain in the next section of this opinion, even if we assume that the search warrant application established probable cause for a search of Pohland's separate apartment, the troopers' search of Pohland's laptop computer was unconstitutional.

Why we conclude that the search of Pohland's laptop computer was unconstitutional

In its brief to this Court, the State argues that the search of Pohland's laptop computer was justified under the principle that a search warrant for a residence generally authorizes the police to search personal effects found within the residence (so long as those containers are capable of concealing the evidence described in the warrant). *See generally LaFave*, § 4.10(b), Vol. 2, p. 946.

The State's argument rests on the premise that Pohland's laptop computer should be viewed as just another personal effect or closed container located in McRoberts's house. For the reasons we are about to explain, we reject this premise.

Portable computing devices — laptop computers, tablets, and smart phones — are distinguishing features of modern life. These devices have changed the way we communicate, and they have changed the way we create and store documents, personal communications and correspondence, photographs, and business records.

The contents of a person's laptop, tablet, or smart phone will often offer a compendium of that person's family and social life, their private and business interests, their recreational activities, and their intimate thoughts. And this digital technology is now practically ubiquitous. According to the Pew Research Center, over 90 percent of Americans own a cell phone, and the rate of computer ownership among adults is roughly 75 percent.[4]

The prevalence of these digital devices has caused courts to re-think the contours of the Fourth Amendment's prohibition against unreasonable searches and seizures. As the United States Supreme Court noted in *Riley v. California*, 573 U.S. __, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014), a police search of this kind of digital device "[will] typically expose to the government far more than the most exhaustive search of a [person's] house", because the device "not only contains in digital form many sensitive records previously found in the home", but also "a broad array of private information never found in a home in any form". *Riley*, 573 U.S. at __, 134 S.Ct. at 2491.

Although *Riley* itself dealt with the search of a cell phone, other courts have recognized that the rationale of *Riley* applies equally to computers and equivalent devices

---

[4] *See* "Technology Device Ownership: 2015" (Oct. 29, 2015), available at: http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015.

for storing electronic data. *See United States v. Turner*, 839 F.3d 429, 434 (5th Cir. 2016); *United States v. Horton*, 863 F.3d 1041, 1047 (8th Cir. 2017), *cert. denied* 138 S.Ct. 1440, 200 L.Ed.2d 721 (2018).

As illustrated by the lengthy discussion that Professor LaFave devotes to this issue — *see LaFave* (5th ed. 2012), § 4.10(d), Vol. 2, pp. 962-971, and the accompanying pocket part (2017), pp. 113-15 — courts have grappled with two related questions: First, what kind of probable cause must a court demand when the police seek authorization to search a personal computer or other digital device? And second, what level of particularity must a court demand when the court issues such a warrant?

Turning to the question of what kind of probable cause was needed to support the seizure and search of Pohland's laptop computer, we note that the search warrant in this case was issued to allow the troopers to search for evidence of crimes committed by *McRoberts* — the suspected crimes of forgery and falsification of business records. The troopers did not assert that Pohland was complicit in McRoberts's forgeries and falsifications of business records. Rather, the troopers' justification for searching Pohland's apartment at all was that *McRoberts* might have concealed evidence of her own wrongdoing inside Pohland's living space.

The warrant authorized the troopers to search for documents "related to the business and finances" of Skye McRoberts and her husband Donavahn. And because business and financial documents nowadays often take digital form, the warrant contained a provision that authorized the troopers to seize and search all the "computers and electronic storage media" within the house for such evidence.

(Technically, the warrant contained a clause that limited this search to only the computers and storage media that were "capable of concealing documents related to the business and finances associated with Donavahn McRoberts or Skye McRoberts". But as a practical matter, this was an authorization to search *every* computer and digital

storage device in the house — because all such devices are "capable" of concealing business and financial documents.)

Putting all of this together, the troopers' rationale for searching Pohland's laptop computer was not because Pohland was suspected of being an accomplice to McRoberts's crimes, but rather because (1) McRoberts was suspected of business and financial wrongdoing, and (2) evidence pertaining to such crimes often takes the form of digital documents, spreadsheets, etc., and (3) McRoberts had physical access to Pohland's living space, and thus (4) McRoberts might have hidden digital evidence of her own crimes on the hard drive of Pohland's laptop.

This kind of speculation did not constitute probable cause to believe that the evidence the troopers were seeking — *i.e.*, documents pertaining to the business and finances of McRoberts and her husband — would be found on Pohland's laptop.

In their search warrant application, the troopers offered no explanation of why they thought that McRoberts could gain access to the hard drive of Pohland's laptop computer, even if McRoberts had physical access to Pohland's living space. The fact that Pohland's laptop was physically located in a rented apartment within McRoberts's house, and the fact that McRoberts was Pohland's landlord and close friend, does not give rise to the inference that McRoberts had access to the contents of the hard drive in Pohland's laptop. Laptop computers are normally equipped with security mechanisms that allow an owner to restrict access to the contents of the laptop by a password or by a similar identification mechanism, such as a fingerprint.

Nor did the troopers offer any explanation of why, even if McRoberts somehow gained access to the laptop's hard drive, McRoberts would choose to hide her business and financial documents on a laptop computer owned by Pohland — a readily portable device that was generally outside McRoberts's immediate control.

The State cites the Ninth Circuit's decision in *United States v. Adjani*, 452 F.3d 1140 (9th Cir. 2006), for the proposition that a search warrant can validly encompass computers and digital storage devices belonging to a third person who shares a house with the target of the investigation. But the facts of *Adjani* differ materially from the facts of Pohland's case.

In *Adjani*, the government was investigating a computer-based crime (extortion by threatening disclosure of a confidential database), and the government's search warrant affidavit expressly asserted that Adjani's girlfriend was involved in the extortion scheme, either as a witting accomplice or at least as an innocent agent who had been duped into performing acts that furthered the scheme. *See Adjani*, 452 F.3d at 1146-47 & n.4. The Ninth Circuit concluded that, in these circumstances, there was probable cause to believe that evidence of Adjani's computer-based crime could be found on his girlfriend's computer. *Ibid.*

In contrast, the search warrant application in Pohland's case did not assert that McRoberts had committed a computer-based crime, nor did it assert that Pohland was actively participating in McRoberts's criminal scheme. And as we have explained, the mere fact that Pohland's laptop was physically located in an apartment within McRoberts's house did not give rise to the inference that McRoberts could access the contents of the laptop's hard drive, nor did it give rise to the inference that McRoberts was likely to hide evidence of her own crimes on a computer that was controlled by Pohland.

Accordingly, we hold that the search warrant application did not establish probable cause to seize and search Pohland's laptop computer.

In addition, we hold that the search warrant in this case failed to satisfy the constitutional requirement of particularity. That is, the warrant failed to limit or restrict the troopers' search of Pohland's laptop so as to reasonably ensure that the troopers

confined their search of the hard drive to those files and folders that were likely to contain the evidence named in the warrant.

Because a modern personal computing device stores and indexes a huge array of information about the private affairs and communications of its owner, all in one place, an authorization to search any and all computing devices and electronic storage devices can easily become the sort of general warrant that the Fourth Amendment was designed to guard against. For this reason, courts have come to recognize that the Fourth Amendment's requirement of "particularity" — *i.e.*, the Fourth Amendment's requirement that a warrant "particularly describ[e] the place to be searched" — is especially important when the police apply for a search warrant that will potentially authorize the search of all the digital devices on a named premises.[5]

This is a situation where "the greatest care in [drafting a search warrant's] description is required", since the likelihood "of [the] seizure of innocent articles by mistake is the most substantial."[6] Accordingly, several courts have condemned warrants that purported to confer "a blanket authorization to search for and seize all electronic

---

[5] *United States v. Otero*, 563 F.3d 1127, 1131-32 (10th Cir. 2009), citing *United States v. Riccardi*, 405 F.3d 852, 863 (10th Cir. 2005), and *United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999).

[6] *LaFave*, § 4.6(a), Vol. 2, p. 774.

devices".[7] Courts have insisted that such warrants provide a reasonably specific description of the material that the police can search for within the device.[8]

In Pohland's case, as we have already explained, the search warrant authorized the troopers to seize and search all the computers and digital storage devices in McRoberts's house for digital business and financial records — more specifically, records related to the business and finances of McRoberts and her husband, to the extent

---

[7] *United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) ("[It is unlawful] to confer a blanket authorization to search for and seize all electronic devices. The warrant must be tailored to the justifications for entering the home. In this case, the warrant should have limited the scope of permissible seizure to devices owned by Griffith, or devices linked to the shooting."); *Commonwealth v. Dorelas*, 43 N.E.3d 306, 312 (Mass. 2016) (Because digital devices contain a wealth of private information, it is not consistent with the Fourth Amendment "to simply permit a search to extend anywhere the [target data] possibly could be found". Rather, "given the properties that render [a computing device] distinct from the closed containers regularly seen in the physical world, a search of its many files must be done with special care", and a warrant to conduct such a search must "satisfy a more narrow and demanding standard.").

[8] *See United States v. Russian*, 848 F.3d 1239, 1245-46 (10th Cir. 2017) (holding that a search warrant for a smart phone was insufficient because it failed to specify the particular material being sought); *State v. Henderson*, 854 N.W.2d 616, 632-34 (Neb. 2014) (invalidating a warrant for the search of a cell phone because the warrant failed to limit the search to the content that was related to the probable cause); *State v. Castagnola*, 46 N.E.3d 638, 657-58 (Ohio 2015) (holding that a search warrant application must be clear as to what the police are seeking on a computing device, and striking down a warrant that permitted the police to examine every record and document on the defendant's computer to find any evidence of the defendant's alleged crimes); *Buckham v. State*, 185 A.3d 1, 18-19 (Del. 2018) (striking down a warrant that authorized the police to search "any and all store[d] data contained within the internal memory" of the defendant's smart phone for evidence of a shooting: "warrants issued to search electronic devices call for particular sensitivity" in light of the "enormous potential for privacy violations" posed by unconstrained searches of these devices).

that these business and financial records were evidence of McRoberts's suspected crimes (forgery and falsification of business records).

The warrant contained no limitation on the kind of search that the troopers could perform on these computers and digital storage devices once they seized them. Instead, the warrant simply authorized the troopers to conduct a "forensic examination" of these digital devices.

And indeed, when the troopers searched Pohland's laptop, they did not restrict their search to "documents related to the business and finances" of Skye McRoberts and her husband. Instead, the troopers conducted a comprehensive examination of the contents of Pohland's laptop. Some of the most important evidence against Pohland was discovered when the troopers found a backup of text messages from Pohland's smart phone. The troopers proceeded to examine thousands of these private text messages, looking for any communication between Pohland and McRoberts.

Because the warrant failed to limit the scope of the troopers' "forensic examination" of Pohland's laptop, the search warrant effectively authorized the troopers to engage in a wide-ranging investigation of Pohland's private affairs. Because of this, the troopers' search of Pohland's laptop exceeded the boundaries of any search that the court might reasonably have authorized, given the information provided in the search warrant application.

For these reasons, we conclude that the search of Pohland's laptop computer violated the Fourth Amendment to the United States Constitution and Article I, Section 14 of the Alaska Constitution. The evidence against Pohland obtained as a result of that search must be suppressed.

Conclusion

The judgement of the district court is REVERSED.