

**NOTICE: SLIP OPINION**  
**(not the court's final written decision)**

The opinion that begins on the next page is a slip opinion. Slip opinions are the written opinions that are originally filed by the court.

A slip opinion is not necessarily the court's final written decision. Slip opinions can be changed by subsequent court orders. For example, a court may issue an order making substantive changes to a slip opinion or publishing for precedential purposes a previously "unpublished" opinion. Additionally, nonsubstantive edits (for style, grammar, citation, format, punctuation, etc.) are made before the opinions that have precedential value are published in the official reports of court decisions: the Washington Reports 2d and the Washington Appellate Reports. An opinion in the official reports replaces the slip opinion as the official opinion of the court.

**The slip opinion that begins on the next page is for a published opinion, and it has since been revised for publication in the printed official reports.** The official text of the court's opinion is found in the advance sheets and the bound volumes of the official reports. Also, an electronic version (intended to mirror the language found in the official reports) of the revised opinion can be found, free of charge, at this website: <https://www.lexisnexis.com/clients/wareports>.

For more information about precedential (published) opinions, nonprecedential (unpublished) opinions, slip opinions, and the official reports, see <https://www.courts.wa.gov/opinions> and the information that is linked there.

**FILED**  
**AUGUST 23, 2018**  
In the Office of the Clerk of Court  
WA State Court of Appeals, Division III

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON  
DIVISION THREE

STATE OF WASHINGTON,	)	
	)	No. 35099-1-III
Respondent,	)	
	)	
v.	)	
	)	
JAY KARL FRIEDRICH,	)	PUBLISHED OPINION
	)	
Appellant.	)	

SIDDOWAY, J. — Anyone engaged in “providing an electronic communication service or a remote computing service” to the public in interstate commerce is required to report any known child pornography violation to an electronic tip line, where it is made available to law enforcement. *See* 18 U.S.C. § 2258A. Jay Friedrich was convicted of five counts of dealing with or possessing depictions of a minor engaged in sexually explicit conduct after Microsoft filed such a report, which was investigated by the Walla Walla County sheriff.

Mr. Friedrich appeals denial of his motion to suppress the critical evidence against him. He argues that the information reported by Microsoft and the warrant affidavit’s generalizations about collectors of child pornography did not provide probable cause for

No. 35099-1-III  
*State v. Friedrich*

a search of his residence and that the affidavit failed to satisfy the particularity required by the Fourth Amendment to the United States Constitution.

The totality of information provided by the affidavit, including commonsense inferences about where and how long child pornography is likely to be retained, provided probable cause to issue the warrant. For that reason, and because any issue of overbreadth is avoided by the severability doctrine, we affirm.

#### FACTS AND PROCEDURAL BACKGROUND

On March 30, 2016, Microsoft reported to the National Center for Missing and Exploited Children (NCMEC)<sup>1</sup> that it became aware that a user of Skype,<sup>2</sup> user name “j kf6418,” uploaded a media file believed to contain a depiction of a minor engaging in sexually explicit conduct. Clerk’s Papers (CP) at 23. Microsoft’s report indicated that a search of Skype for the username “j kf6418” yielded three results, all belonging to a “Jay Friedrich.” *Id.* The one result identifying “Jay Friedrich[’s]” city of residence identified it as Walla Walla, Washington. The NCMEC report indicated that a search of the

---

<sup>1</sup> NCMEC is a national resource center and clearinghouse that maintains an electronic tip line, the “CyberTipline,” through which federally-required reports are transmitted to the appropriate international, federal, and local law enforcement agencies for investigation. 42 U.S.C. §§ 5771, 5773(b). Providers who fail to comply with the reporting obligation face substantial penalties. *See* 18 U.S.C. § 2258A; *United States v. Ackerman*, 831 F.3d 1292, 1296-97 (10th Cir. 2016).

<sup>2</sup> Skype is a telecommunications application for video chats, voice calls, or instant messaging. *See About Skype*, SKYPE, <https://www.skype.com/en/about> [<https://perma.cc/LL58-566K>].

No. 35099-1-III  
*State v. Friedrich*

username “jkf6418” on Spokeo, a people search website that aggregates data from other services, also yielded three results. One, a dating profile on an online dating site, described “jkf6418” as a 51-year-old bisexual single male from Walla Walla and as 6’1” and of average build.

After it was determined that the Internet Protocol (IP) address most likely came from Walla Walla, the information was passed along to the Walla Walla County Sheriff’s Department and investigation of the report was referred to Detective Eric Knudson on April 12. Detective Knudson viewed the media file, a picture of what appeared to be an approximately 9- to 11-year-old girl engaged in “sexually explicit . . . conduct” as defined by RCW 9.68A.011(4). CP at 24.

On April 13, Detective Knudson obtained a search warrant to locate the subscriber information for the IP address, which was registered to Charter Communications. Charter Communications responded to the warrant on April 21, identifying the service subscriber as Jay Jensen. Detective Knudson learned from a search of police records that in 2012 Jay Jensen reported finding child pornography on his roommate’s computer. The report listed Mr. Jensen’s roommate as Jay Friedrich. Mr. Friedrich was not charged as a result of that report, as the investigation produced insufficient evidence for prosecution. Detective Knudson nonetheless reviewed the pictures obtained in the investigation and determined that they were of teenage and preteen girls. Detective Knudson’s research also revealed that Mr. Friedrich is a registered sex offender.

No. 35099-1-III  
*State v. Friedrich*

Detective Knudson learned from police records that Mr. Friedrich lived in Walla Walla and was described as 52 years of age, 6’1” in height, and as weighing 155 pounds. His birthdate was recorded as 04/18/1964, which, along with his initials, jkf, correlated to the “jkf6418” account (04/18/1964).

A month after NCMEC received the report from Microsoft, on April 27, Detective Knudson applied for a warrant to search Mr. Friedrich’s residence. In his 24-page supporting affidavit, Detective Knudson provided his background and training, the foregoing information, and information on the typical operational practices of electronic and internet service providers (collectively “ISPs”). He testified that pursuant to terms of their user agreements, ISPs “typically monitor their services utilized by subscribers[ t]o prevent their communication networks from serving as conduits for illicit activity” and “routinely and systematically attempt to identify suspected child pornography that may be sent through [the ISP’s] facilities.” CP at 17. He testified that when an image or video file is believed by an ISP to be child pornography as defined by 18 U.S.C. § 2256, a “hash value” of the file can be generated by operation of a mathematical algorithm that is unique to the file—“in essence, the unique fingerprint of that file.” CP at 17. A database of hash values for files suspected to be child pornography enables ISPs to automatically detect when files that have been identified as illicit pass through their system. He testified that reports to NCMEC by ISPs are often made solely on the basis of detection of a file’s hash value.

No. 35099-1-III  
*State v. Friedrich*

In addition to describing these practices (although in more detail), Detective Knudson’s affidavit stated that under federal law, an ISP “has a duty to report to NCMEC any apparent child pornography it discovers ‘as soon as reasonably possible.’” CP at 18 (quoting 18 U.S.C. § 2258A(a)(1)).

The items that Detective Knudson sought to search for and seize were identified in two single-spaced pages of an attachment to his affidavit. They consisted of two categories: “Records, Documents, and Visual Depictions,” and “Digital Evidence.” CP at 32-33.

The requested search warrant was issued by District Court Judge Kristian Hedine on April 27. The last, freestanding provision of its digital evidence section authorized the seizure of records and things evidencing the use of nine IP addresses that were unrelated to Microsoft’s report to NCMEC. They were not identified or explained by Detective Knudson’s affidavit or its attachments.

In executing the search warrant the next day, law enforcement seized a Hewlett Packard laptop, a Toshiba laptop, a Micron tower computer, flash drives, compact disks, and floppy disks—all found in Mr. Friedrich’s bedroom. They seized a Samsung smartphone from Mr. Friedrich’s person. During an interview with officers, Mr. Friedrich admitted that the electronics seized were his and that they would contain images of underage girls. The Hewlett Packard computer and the Samsung smartphone proved to contain depictions of minors engaged in sexually explicit conduct, including

No. 35099-1-III  
*State v. Friedrich*

the image Microsoft reported. The Toshiba laptop and Micron tower computer also contained such depictions.

The State eventually charged Mr. Friedrich with one count of second degree dealing in depictions of a minor engaged in sexually explicit conduct, three counts of first degree possession of depictions of a minor engaged in sexually explicit conduct, and one count of second degree possession of depictions of a minor engaged in sexually explicit conduct, all in violation of RCW 9.68A.050 and .070. For simplicity's sake hereafter, and unless indicated otherwise, our references to "child pornography" are to depictions of minors whose possession or dealings with which violate provisions of chapter 9.68A RCW or federal law.

Mr. Friedrich moved the court to suppress all of the State's evidence, arguing that Detective Knudson's affidavit supporting his application did not meet the particularity requirement of the Fourth Amendment. The superior court, the Hon. John Lohrmann, denied the motion without a hearing. The parties then proceeded to a stipulated facts trial, with Mr. Friedrich preserving his right to appeal the trial court's suppression decision. Mr. Friedrich was convicted on all remaining counts. He appeals.

#### ANALYSIS

Mr. Friedrich's assignments of error present two challenges to the trial court's suppression decision. He contends first, that the warrant application failed to provide facts supporting a determination that what was at least month-old evidence of criminal

No. 35099-1-III  
*State v. Friedrich*

activity could still be found at his residence. His second contention is that the search warrant failed to satisfy the particularity requirement of the Fourth Amendment.

I. THE DISTRICT COURT COULD REASONABLY CONCLUDE THAT THE EVIDENCE OF CRIMINAL ACTIVITY WAS NOT STALE

Mr. Friedrich does not question that the warrant affidavit provided probable cause that he engaged in criminal activity at some time. But he cites two aspects of Detective Knudson’s affidavit that he argues undermine probable cause that evidence of the criminal activity existed at Mr. Friedrich’s residence at the time the detective applied for the search warrant. The first is the fact that the March 30, 2016 date of Microsoft’s report to the CyberTipline was the date Microsoft “*became aware* that a user uploaded a media file,” not the date of the upload itself. CP at 23 (emphasis added). The second is that four weeks had passed between Microsoft’s report and the application for the warrant, and the detective’s contention that the evidence would still be at the residence depended on unreliable generalizations about the habits of child pornography collectors.

The Fourth Amendment to the United States Constitution and article I, section 7 of the Washington Constitution require that the issuance of a search warrant be based on a determination of probable cause. Probable cause is established when an affidavit supporting a search warrant provides sufficient facts for a reasonable person to conclude there is a probability the defendant is involved in the criminal activity and that evidence



No. 35099-1-III  
*State v. Friedrich*

of the crime is at a certain location. *State v. Vickers*, 148 Wn.2d 91, 108, 59 P.3d 58 (2002).

Whether a warrant affidavit's information constitutes probable cause is a question of law that we review de novo. *State v. Neth*, 165 Wn.2d 177, 182, 196 P.3d 658 (2008). Nonetheless, in determining that question of law, “[g]reat deference is accorded the issuing magistrate’s determination of probable cause.” *State v. Cord*, 103 Wn.2d 361, 366, 693 P.2d 81 (1985). If the propriety of issuing the warrant is debatable, the deference due the magistrate’s decision will tip the balance in favor of upholding the warrant. *State v. Jackson*, 102 Wn.2d 432, 446, 688 P.2d 136 (1984). In light of the deference owed the magistrate’s decision, the question on review is whether the magistrate could draw the connection, not whether he should do so.

In reviewing a magistrate’s determination of probable cause, we—like the magistrate—should not view the affidavit “in a hypertechnical manner.” *State v. Riley*, 34 Wn. App. 529, 531, 663 P.2d 145 (1983). “[A] magistrate is entitled to draw reasonable inferences from the facts and circumstances set forth in the supporting affidavit,” with the result that “[r]easonableness is the key and common sense must be the ultimate yardstick.” *Id.* “Doubts concerning the existence of probable cause are generally resolved in favor of issuing the search warrant.” *Vickers*, 148 Wn.2d at 108-09.

No. 35099-1-III  
*State v. Friedrich*

*Timeliness of Microsoft's detection and report*

A passage of time between an observation of criminal activity and the presentation of a search warrant affidavit may be so prolonged that it is no longer probable that a search will reveal criminal activity or evidence; i.e., the information may be stale. *State v. Lyons*, 174 Wn.2d 354, 360-61, 275 P.3d 314 (2012). But “the information is not stale for purposes of probable cause if the facts and circumstances in the affidavit support a commonsense determination that there is continuing and contemporaneous possession of the property intended to be seized.” *State v. Maddox*, 152 Wn.2d 499, 506, 98 P.3d 1199 (2004).

Detective Knudson's affidavit stated that Microsoft's report indicated that it “became aware” of Mr. Friedrich's upload on March 30. CP at 23. It also informed the magistrate that ISPs such as Microsoft typically monitor their services to prevent their communication networks from serving as conduits for illicit activity, including to systematically attempt to identify suspected child pornography. He described the generation of hash values for pornographic files that enable ISPs to automatically detect the passage of some pornographic files through their system. Detective Knudson also cited federal law under which an ISP “has a duty to report to NCMEC any apparent child pornography it discovers ‘as soon as reasonably possible.’” CP at 18 (quoting 18 U.S.C. § 2258A(a)(1)). Mr. Friedrich concedes that “[p]resumably, Microsoft complied with this requirement.” Br. of Appellant at 15 n.11.

No. 35099-1-III  
*State v. Friedrich*

Industry practices exist, can often be determined by outsiders to the industry, and the practices described by Detective Knudson's affidavit are matters of which a detective with training in investigating child pornography cases could be expected to be aware. The district court judge was entitled to rely on the detective's knowledge of industry practice. That information and the federal reporting requirement support the magistrate's commonsense conclusion that Microsoft's detection and reporting would be prompt.

*Likelihood that evidence of criminal activity would be located at Mr. Friedrich's residence*

To establish the likelihood that evidence of criminal activity would still be located at Mr. Friedrich's residence, Detective Knudson's affidavit relied in part on the fact that digitized information will remain on a computer not only until deleted, but even thereafter, which Mr. Friedrich does not dispute.

Detective Knudson's affidavit also included generalizations about what collectors of child pornography generally do, which, according to the deputy, includes "prefer[ing] not to be without their child pornography for any prolonged time period," often maintaining photographs or videos "in computer files or external digital storage devices," and maintaining pornographic materials "in the privacy and security of their home or in some other secure location, such as a private office." CP at 14-15. Mr. Friedrich challenges these generalizations as support for a determination of probable cause, citing *State v. Thein*, 138 Wn.2d 133, 977 P.2d 582 (1999).

No. 35099-1-III  
*State v. Friedrich*

In *Thein*, our Supreme Court held that an officer's asserted understanding of the common habits of drug dealers was insufficient to establish probable cause to search the defendant's residence. The warrant affidavit in *Thein* presented specific facts providing probable cause that the defendant was a drug dealer, but only generalizations in support of the officer's belief that evidence of his criminal activity could be found at his residence. The court concluded that the generalized statements "in [Thein's] case were, standing alone, insufficient to establish probable cause to search [his] residence." *Id.* at 148. Although allowing that "common sense and experience inform the inferences reasonably to be drawn from the facts," the Court determined that the type of "broad generalizations" presented by the warrant affidavit for Thein's residence "do not alone establish probable cause." *Id.* at 148-49.

The Court added a cautionary note, "emphasiz[ing] that the existence of probable cause is to be evaluated on a case-by-case basis" and in each case, "'the facts stated, the inferences to be drawn, and the specificity required must fall within the ambit of reasonableness.'" *Id.* at 149 (quoting *State v. Helmka*, 86 Wn.2d 91, 93, 542 P.2d 115 (1975)). More recently, our Supreme Court observed in *Maddox* that "[i]n evaluating whether the facts underlying a search warrant are stale, the court looks at the totality of circumstances," including "the nature and scope of the suspected criminal activity." 152 Wn.2d at 506.

Detective Knudson's generalizations about what possessors of child pornography

No. 35099-1-III  
*State v. Friedrich*

“generally do” warrant critical examination for the reasons given in *Thein*. But unlike the generalizations about drug dealers in *Thein*, Detective Knudson’s generalizations about possessors of child pornography fall within the ambit of reasonableness, and similar generalizations have survived critical examination in a number of courts. In a relatively early case involving a warrant to search for digital evidence of child pornography at a user’s residence, the federal appellate court for the Tenth Circuit Court of Appeals endorsed a view that possessors of child pornography are likely to hoard materials and maintain them for significant periods of time, explaining that the view

“is supported by common sense and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence.”

*United States v. Riccardi*, 405 F.3d 852, 861 (10th Cir. 2005) (quoting *United States v. Lamb*, 945 F. Supp. 441, 460 (N.D.N.Y. 1996)).

The Tenth Circuit abided by that view five years later, despite an intervening increase in internet access to child pornography that made it easier to anonymously collect and possess it. In *United States v. Burkhart*, the court explained:

[C]hild pornography is still illegal to distribute and possess, and still carries severe social stigma, whether the possessor receives it by regular mail, email, or over the Internet. The illegality and social stigma may also complicate resale or disposal. Moreover, acquiring pornography is rarely free. Given the nature of the evidence to be seized, the Internet context may mitigate *against* staleness: information that a person received

No. 35099-1-III  
*State v. Friedrich*

electronic images of child pornography is less likely than information about drugs, for example, to go stale because the electronic images are not subject to spoilage or consumption.

602 F.3d 1202, 1207 (10th Cir. 2010) (citing *United States v. Frechette*, 583 F.3d 374, 378 (6th Cir. 2009)). *Burkhart* points out that at the time of its filing, it was one of five federal circuit courts that had endorsed the observation that possessors of child pornography are likely to hoard it. *Id.*<sup>3</sup> This court also found that “boilerplate” inferences in a warrant affidavit provided probable cause that evidence of child pornography could be found at a suspect’s residence months after detecting his use. *State v. Garbaccio*, 151 Wn. App. 716, 729, 214 P.3d 168 (2009), relying on *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997).

Probable cause requires more than suspicion or conjecture, but it does not require certainty. *State v. Chenoweth*, 160 Wn.2d 454, 476, 158 P.3d 595 (2007). Because common sense and experience supports the generalizations presented by Detective Knudson, the district court could reasonably find a fair probability that possessors of child pornography are likely to retain the material for a considerable period of time in a secure location, such as the possessor’s home.

---

<sup>3</sup> In addition to the Sixth Circuit decision in *Frechette*, *Burkhart* cited *United States v. McArthur*, 573 F.3d 608, 613-14 (8th Cir. 2009); *United States v. Falso*, 544 F.3d 110, 132 (2d Cir. 2008); and *United States v. Watzman*, 486 F.3d 1004, 1008 (7th Cir. 2007).

No. 35099-1-III  
*State v. Friedrich*

II. THE SEARCH WARRANT SATISFIED THE CONSTITUTIONAL PARTICULARITY REQUIREMENT IN MOST RESPECTS, AND THE ITEMS SEIZED FALL WITHIN ITS LEGITIMATE SCOPE

Mr. Friedrich’s remaining argument is that the search warrant was vague, overbroad, and sought materials presumptively protected by the First Amendment to the United States Constitution.

Among the requirements of the Fourth Amendment is that no warrant shall issue without “*particularly describing* the place to be searched, and the persons or things to be seized.” U.S. CONST. AMEND. IV (emphasis added); *State v. Riley*, 121 Wn.2d 22, 28 n.1, 846 P.2d 1365 (1993). “The purposes of the search warrant particularity requirement are the prevention of general searches, prevention of the seizure of objects on the mistaken assumption that they fall within the issuing magistrate’s authorization, and prevention of the issuance of warrants on loose, vague, or doubtful bases of fact.” *State v. Perrone*, 119 Wn.2d 538, 545, 834 P.2d 611 (1992) (citing, among other authority, *Marron v. United States*, 275 U.S. 192, 48 S. Ct. 74, 72 L. Ed. 231 (1927)).

The first two purposes are related. The first prevents the sort of general, exploratory rummaging in a person’s belongings of the sort “‘abhorred by the colonists.’” *Id.* (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971)). The second ensures that what is to be seized is determined by a neutral magistrate, eliminating the danger of unlimited discretion in the executing officer. *Id.* at 546. As to these related purposes, “a description is valid if it is as specific as the

No. 35099-1-III  
*State v. Friedrich*

circumstances and the nature of the activity under investigation permits.” *Perrone*, 119 Wn.2d at 547.

A greater degree of particularity is required when a search warrant authorizes a search for items protected by the First Amendment. *Id.* at 547. Describing the history of this heightened requirement in 1965, the U.S. Supreme Court stated that “[T]he most scrupulous exactitude” applies “when the ‘things [to be seized]’ are books, and the basis for their seizure is the ideas which they contain.” *Stanford v. Texas*, 379 U.S. 476, 485, 85 S. Ct. 506, 13 L. Ed. 2d 431 (cited by *Perrone*, 119 Wn.2d at 547-48).

The third purpose of the particularity requirement ties it to the requirement of probable cause. Imprecision in the description of the items to be seized that can be traced to “loose, vague, or doubtful bases of fact” increases the likelihood that probable cause has not been established. *Perrone*, 119 Wn.2d at 548. As to all three purposes, “[w]hether a search warrant contains a sufficiently particularized description is reviewed de novo.” *Id.* at 549.

The first infirmity alleged by Mr. Friedrich for his particularity challenge is the search warrant’s use of the unqualified term “child pornography” in one instance, in describing items to be seized. Use of the unqualified term proved fatal to the search warrant at issue in *Perrone*, in which the warrant affidavit repeatedly used the term to describe items to be seized, and our Supreme Court held that the term was “not sufficiently particular to satisfy the Fourth Amendment.” 119 Wn.2d at 553. The court



No. 35099-1-III  
*State v. Friedrich*

reasoned that authorizing law enforcement to seize anything it thinks constitutes “child pornography” allows for too much discretion and is not “scrupulous exactitude.” *Id.* (internal quotation marks omitted). The court suggested that a warrant affiant could avoid the particularity problem by using statutory definitions found in RCW 9.68A.011.<sup>4</sup> *Id.* at 553-54. More recently, the Court reiterated that if a search warrant limiting items to be seized “used the *language* of RCW 9.68A.011 to describe materials sought, the warrant would likely be sufficiently particular,” but that merely identifying the crime under investigation as a violation of RCW 9.68A.070 did not satisfy the particularity requirement. *State v. Besola*, 184 Wn.2d 605, 614, 359 P.3d 799 (2015).

The search warrant in this case consistently qualified the “Records, Documents, and Visual Depictions” to be searched for and seized as ones containing, or pertaining or relating to, “visual depictions of minors engaged in sexually explicit conduct, as defined in RCW 9.68A.011 and Title 18, United States Code, Section 2256.” CP at 32. All items to be searched and seized were also qualified by introductory language that they be “records, documents, and items that constitute evidence, contraband, fruits, and/or instrumentalities of violations of RCW 9.68A.050, dealing in depictions of minor [sic] engaged in sexually explicit conduct.” CP at 35. The unqualified term “child

---

<sup>4</sup> Chapter 9.68A RCW covers sexual exploitation of children, and section 9.68A.011 is its definitions provision.

No. 35099-1-III  
*State v. Friedrich*

pornography” appears only once, in authorizing seizure of materials “that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess or view child pornography.”

CP at 37. Given the introductory language and the consistent use of statutory definitions elsewhere, Mr. Friedrich’s attack is hypertechnical. The search warrant in this case does not present the infirmity presented by the search warrant in *Perrone*.

Additional and related infirmities alleged by Mr. Friedrich are the breadth of the media to be seized, which includes, e.g., books, magazines, photographs, motion picture films and videos; and the warrant’s extension to every digital device found in the residence that is “capable of storing and/or processing data in digital form,” as well as “related communications devices,” examples of which are provided. CP at 36. He argues that the breadth of both categories authorizes the seizure of items unrelated to the suspected crime, which was a single instance of uploading a digital image. Finally, he points to the fact that the search warrant authorized seizure of records and things evidencing the use of nine IP addresses having no apparent relation to Detective Knudson’s evidence.

The State responds that the particularity requirement tolerates ambiguity when the description is as complete as can be reasonably expected, and that the complaint about the breadth of devices whose seizure was authorized fails to consider that “[t]he only way police will know whether digital evidence contains child pornography is by seizing the

No. 35099-1-III  
*State v. Friedrich*

device and then submitting it to . . . expert examination. This cannot be ascertained at the time of seizure.” Br. of Resp’t at 19-20.

The State does not defend the provision of the search warrant dealing with the nine unexplained IP addresses, lending credence to Mr. Friedrich’s surmise that it was carryover language from an earlier search warrant. We set aside that provision for now, and address it in our concluding discussion of the severability doctrine.

As to the breadth of the types of media to be seized, “courts evaluating alleged particularity violations have distinguished between property that is inherently innocuous and property that is inherently illegal.” *State v. Chambers*, 88 Wn. App. 640, 644, 945 P.2d 1172 (1997) (internal quotation marks omitted). “A lesser degree of precision may satisfy the particularity requirement when a warrant authorizes the search for contraband or inherently illicit property.” *Id.* Child pornography is not protected by the First Amendment. *New York v. Ferber*, 458 U.S. 747, 102 S. Ct. 3348, 73 L. Ed. 2d 1113 (1982). The search warrant authorized a search for and seizure of only media containing statutorily-defined child pornography. It was not overbroad as to media whose content could be assessed during the search.

The breadth of digital devices to be seized presents a different issue because, as the State points out, whether they contained child pornography could not be assessed while executing the warrant at the residence. If a magistrate reasonably finds it probable that an individual has engaged in criminal dealings with child pornography, and digital

No. 35099-1-III  
*State v. Friedrich*

evidence of those dealings is likely to be found in devices located in his or her home, the most reasonable approach would appear to be to authorize seizure of all reasonably suspect devices, but with a particularized protocol for searching the devices following the seizure. *See, e.g., United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (per curiam) (en banc) (recognizing “the reality that over-seizing is an inherent part of the electronic search process”), *abrogated in part on other grounds by Hamer v. Neigh. Hous. Serv. Of Chi.*, \_\_\_ U.S. \_\_\_, 138 S. Ct. 13, 16-17, 199 L. Ed. 2d 249 (2017); *id.* at 1178-80 (Kozinski, C.J., concurring) (providing guidance on what magistrates should consider in issuing a warrant to examine an electronic storage medium to search for certain incriminating files).

The severability doctrine spares us the task of drawing lines about over-seizing electronic information in this case, because the evidence that was seized and used to convict Mr. Friedrich was seized pursuant to provisions of the warrant that were particularized and supported by probable cause.<sup>5</sup> Under the severability doctrine, which “has been applied [even] where First Amendment considerations exist,” “‘infirmity of part of a warrant requires the suppression of evidence seized pursuant to that part of the warrant’ but does not require suppression of anything seized pursuant to valid parts of the warrant.” *Perrone*, 119 Wn.2d at 556 (quoting *United States v. Fitzgerald*, 724 F.2d 633,

---

<sup>5</sup> The evidence relied on by the State was found on the Hewlett Packard computer, the Samsung smartphone, the Toshiba computer, and the Micron computer.

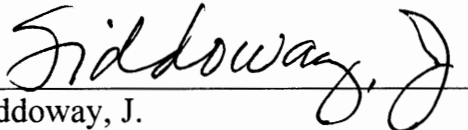
No. 35099-1-III  
*State v. Friedrich*

warrant.” *Perrone*, 119 Wn.2d at 556 (quoting *United States v. Fitzgerald*, 724 F.2d 633, 637 (8th Cir. 1983)). Although the doctrine does not apply to unconstitutional general warrants or where the valid portion of the warrant is “a relatively insignificant part of an otherwise invalid search,” *id.* at 556-57 (internal quotation marks omitted), neither of those exceptions to the doctrine apply here.

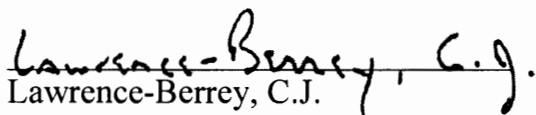
The warrant was not too vague and did not authorize the seizure of items protected by the First Amendment. Its extension to nine unrelated IP addresses and any other debatable overbreadth did not taint its valid and severable authorization to seize the three computers and one smartphone relied on as evidence against Mr. Friedrich.

Mr. Friedrich asks us to exercise our discretion to waive costs on appeal if the State substantially prevails, which it has. We decline to exercise our discretion to waive costs, but this does not prejudice Mr. Friedrich’s right to oppose an award of costs under RAP 14.2.

Affirmed.

  
Siddoway, J.

WE CONCUR:

  
Lawrence-Berrey, C.J.

No. 35099-1-III

FEARING, J. (concurring) — The majority writes, on page 8 of its opinion:

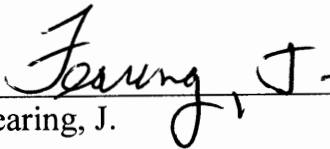
Whether a warrant affidavit's information constitutes probable cause is a question of law that we review de novo. *State v. Neth*, 165 Wn.2d 177, 182, 196 P.3d 658 (2008). Nonetheless, in determining that question of law, "[g]reat deference is accorded the issuing magistrate's determination of probable cause." *State v. Cord*, 103 Wn.2d 361, 366, 693 P.2d 81 (1985). If the propriety of issuing the warrant is debatable, the deference due the magistrate's decision will tip the balance in favor of upholding the warrant. *State v. Jackson*, 102 Wn.2d 432, 446, 688 P.2d 136 (1984). In light of the deference owed the magistrate's decision, the question on review is whether the magistrate could draw the connection, not whether he should do so.

I question the consistency of the first sentence in this excerpt from the remaining sentences. A de novo review may conflict with granting the magistrate deference, let alone great deference. Perhaps the appeals court should grant deference only to the extent the magistrate needed to determine the reliability of information submitted in support of the application for a search warrant and not to the extent of deciding whether that information supported probable cause. I also question whether a reviewing court should grant the magistrate deference when the magistrate issues the search warrant without any input from the defendant.

No. 35099-1-III

*State v. Friedrich* (concurrency)

In another case, a court may need to resolve the discrepancy between the principle of de novo review and the rule of granting the magistrate deference. The majority and I need not undertake any resolution of this incongruity in this appeal, because under either standard of review, we may affirm the issuance of the warrant to search Jay Friedrich's residence.

  
Fearing, J.