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may issue an order making substantive changes to a slip opinion or publishing for precedential purposes a previously "unpublished" opinion.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For more information about precedential (published) opinions, nonprecedential (unpublished) opinions, slip opinions, and the official reports, see https://www.courts.wa.gov/opinions and the information that is linked there.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
OCTOBER 4, 2022
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, Respondent, v. MICHAEL E. CHAMBERS, Appellant.	)))))))))	No. 38282-6-III OPINION PUBLISHED IN PART

STAAB, J. — An internet crime unit investigation in Idaho determined that an internet protocol (IP) address registered to Michael Chambers in nearby Asotin County was downloading and sharing depictions of minors engaged in sexually explicit conduct. Following a stipulated bench trial, Chambers was convicted of 24 counts of first degree possession, two counts of first degree dealing, and one count of second degree dealing in depictions of a minor engaged in sexually explicit conduct. He raises six issues on appeal. In the published portion of this decision, we reject Chambers' postverdict challenge to the adequacy of the information. We also hold that the presence and participation of Idaho police, at the request of a Washington deputy, to aid in the execution of the search warrant was not prohibited by statute and was otherwise

authorized by common law.

In the unpublished portion of the decision, we hold that the search warrant was supported by probable cause and not overbroad. We find that the evidence was sufficient to support a finding of intent to distribute for purposes of counts 1, 2, and 3. We affirm imposition of the polygraph condition as part of Chambers' community custody condition, but strike the overbroad internet condition and remand for reconsideration of this sentencing condition.

BACKGROUND

We provide a brief overview of the facts and procedure here. Additional details are set forth in the discussion of each issue.

On September 30, 2017, and October 1, 2017, Detective Eric Kjorness of the Moscow Police Department Internet Crimes Against Children (ICAC) unit was using computer peer-to-peer (P2P) file sharing software (often referred to as "BitTorrent") to conduct a broad sweep investigation of internet child pornography trafficking by accessing other BitTorrent users' open and available computer files. Clerk's Papers (CP) at 259. P2P file sharing is a method of communication available to internet users through the use of special software that links their computers through a network and allows for the sharing of digital files directly between users on the network. After obtaining the

software by download, a user can set up file(s) on his/her computer to be shared with others running compatible P2P software.

> BitTorrent, one type of P2P software, sets up its searches by keywords typically on torrent websites. The results of a keyword search are displayed to the user. The website does not contain the files being shared, only file[s] referred to as a "torrent." The user then selects a torrent file(s) from the results for download. . . . The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the actual files (not the torrent file but the actual files referenced in the torrent file using any BitTorrent client.).

CP at 112. More than one file can be downloaded at once, and a user may download parts of files from more than one source computer at a time for integration.

This transfer is assisted by reference to a unique IP address expressed as four numbers separated by decimal points assigned to a particular computer during an online session. Every computer attached to the internet is assigned an IP address to assure proper direction of data. Most internet service providers control the range of assigned IP addresses. Some IP addresses are "static" long-term assignments and others have "dynamic" addresses that are frequently changed. CP at 117. "BitTorrent users are able to see the IP address of any computer system sharing files to them or receiving files from them. Investigators log the IP address which were sent files or information regarding files being shared." CP at 113. Using the "American Register of Internet Numbers," investigators can determine the internet service provider assigned that IP address. CP at

113. The specific computer assigned to the IP address can then be obtained from the internet service provider.

During his investigation, Detective Kjorness was able to identify a specific IP address that was downloading and sharing known images of depictions of minors engaged in sexually explicit conduct. The IP address was assigned to an internet provider, CableOne, out of Lewiston, Idaho. Responding to a subpoena, CableOne indicated the IP address was assigned to an account in Chambers' name with an Asotin County address. Based on his findings, Detective Kjorness contacted Detective Brian Birdsell of the Lewiston Police Department, who in turn contacted Detective Jackie Nichols of the Asotin County Sheriff's Office on October 30, 2017. Detective Nichols obtained a search warrant from the Asotin County Superior Court for Chambers' home in Clarkston, Washington.

On December 21, 2017, Detective Nichols executed the warrant with the assistance of law enforcement officers from several agencies including Detective Kjorness of the Moscow, Idaho, police department. Detective Nichols testified at the suppression motion that as a rural officer, she has generalized training, but to fill the void in her experience, she utilizes assistance from outside agencies. She invited Detective

Kjorness to assist with the execution of the Chambers' warrant because the detective is an expert in this field.

During execution of the search warrant, Detective Kjorness questioned Chambers about his technical expertise and the presence of child pornography on his system and performed preliminary searches of two tower computers. Detective Nichols was present when Detective Kjorness spoke to Chambers. Chambers made significant incriminating statements during the execution of the search warrant particularly that he installed and used a BitTorrent program called "Azureus," downloaded sexually explicit images of children, saw them, and did not delete them because he was trying to help the police investigate. CP at 31-33. He knew that he should not be doing it. He did not turn anything over to police because he did not think that he had anything helpful.

Chambers claimed to not be sharing images but when confronted with a claim that he had made them available over his BitTorrent program, he responded that he "thought he 'had the outgoing totally shut down.'" CP at 38. He commented, "'Wow. My bad there.'" CP at 38. He admitted to going to online sources that he knew contained sexual images of children. He repeatedly denied distributing any images.

Detective Nichols delivered all of the digital devices seized from the home to Detective Birdsell for forensic analysis on December 26, 2017. The evidence was

returned to Asotin County on May 9, 2018. Detective Birdsell identified a large quantity of sexually explicit images depicting children (6,314), and confirmed that Chambers' computer hard drives used by default the same MAC (media access control) address listed on the CableOne record.

Asotin County charged Chambers with two counts of "Dealing in Depictions of Minor Engaged in Sexually Explicit Conduct in the First Degree" and one count of "Dealing in Depictions of Minor Engaged in Sexually Explicit Conduct in the Second Degree" in violation of RCW 9.68A.050(1) and (2). CP at 1-3. He was also charged with 24 counts of "Possession of Depictions of Minor Engaged in Sexually Explicit Conduct in the First Degree" in violation of RCW 9.68A.070(1). CP at 4-27.

Chambers filed several motions to suppress evidence. Ultimately, the trial judge denied his motions to suppress evidence seized from the house, but granted the motions to suppress evidence seized from an adjacent shop that was not described in the affidavit or included in the search warrant. Following the court's decision, Chambers elected to proceed to a bench trial on stipulated facts.

The stipulated evidence included 28 digital files retrieved from computers located in Chambers' home. Explicit descriptions of these videos and images were provided by

Detective Birdsell and included in the stipulated evidence. Chambers stipulated that Detective Birdsell's descriptions were accurate and sufficient.

Chambers was found guilty on all counts and sentenced. His judgment and sentence contained conditions prohibiting internet access and submission to polygraph tests. The precise wording is included below.

During his sentencing statement, Chambers admitted to intentionally setting his BitTorrent upload speed to slow, indicating his knowledge that he was disseminating, and described himself as a "hacker" capable of hex editing. CP at 330-31.

Chambers timely appealed.

ANALYSIS

A. POSTVERDICT CHALLENGE TO THE INFORMATION

In his first issue on appeal, Chambers challenges the sufficiency of the information charging him with 3 counts of disseminating, and 24 counts of possession of images depicting a minor engaged in sexually explicit conduct. Chambers argues these offenses require not only that the State prove knowledge of the act (possession or disseminating) but also knowledge of the nature of the depictions. He contends that the charging information failed to allege the second scienter element. We review this legal challenge de novo. *State v. Goss*, 186 Wn.2d 372, 376, 378 P.3d 154 (2016).

An information must allege each essential element, statutory and otherwise, to apprise the accused of the charges against him or her and to allow for preparation of a defense. *State v. Vangerpen*, 125 Wn.2d 782, 787, 888 P.2d 1177 (1995). The information must do more than merely list the offense, but it need not restate the precise language of the criminal statute. *State v. Nonog*, 169 Wn.2d 220, 226, 237 P.3d 250 (2010). "[I]t is sufficient if words conveying the same meaning and import are used." *State v. Kjorsvik*, 117 Wn.2d 93, 108, 812 P.2d 86 (1991).

Chambers did not challenge the information before a verdict was reached. While a constitutional challenge to the charging document can be raised for the first time on appeal, the late objection changes the level of deference we apply. *Id.* at 102. "When, as in this case, a charging document is challenged for the first time on appeal, we construe it liberally." *State v. Pry*, 194 Wn.2d 745, 752, 452 P.3d 536 (2019). Under this standard, we consider the charging document as a whole and in a commonsense manner to determine if the implied element can be fairly inferred through a liberal construction in favor of its validity. *Kjorsvik*, 117 Wn.2d at 110-11. Under the two-pronged test developed by *Kjorsvik*, our first question is whether the essential elements appear in any form or by fair construction can be found. *Id*. at 105. If so, we consider whether the defendant can show actual prejudice by language used that caused a lack of notice. *Id*. at

106. However, if the information fails to meet the first prong, prejudice is presumed and requires reversal. *State v. Zillyette*, 178 Wn.2d 153, 162, 307 P.3d 712 (2013).

The State's charging information used the verbatim language of the statutes, RCW 9.68A.050 and RCW 9.68A.070. As to the disseminating charges, counts 1 through 3, the information charged that Chambers "knowingly developed, duplicated, published, disseminated, or exchanged or possessed with intent to develop, duplicate, publish, disseminate, or exchange visual or printed matter depicting a minor engaged in sexually explicit conduct . . . ." CP at 1-3; *see* RCW 9.68A.050(1)(a)(i). Similarly, with respect to the possession charges, the information alleged that Chambers "knowingly possessed visual or printed matter depicting a minor engaged in sexually explicit conduct . . . ." CP at 4-27; *see* RCW 9.68A.070(1)(a).

Chambers contends the statutory language used in the information has already been found to be constitutionally insufficient. In *State v. Rosul*, the Supreme Court addressed the defendant's overbreadth challenge to the child pornography statutes. 95 Wn. App. 175, 182, 974 P.2d 916 (1999). Against this First Amendment to the United States Constitution backdrop, the court found that "[a] natural grammatical reading of RCW 9.68A.070 would apply the scienter requirement to possession, but not to the age of the children depicted." *Id*. After finding that such a scienter requirement was necessary

to preserve the constitutionality of the statute, the court construed the statute to require a showing that the defendant was aware of the general nature of the material he possessed. *Id*. at 185. Following *Rosul*, the statutes are now construed to require "a showing that the defendant was aware not only of possession, but also of the general nature of the material he or she possessed." *Id*.

Chambers argues that *Rosul*'s "natural reading" of the statute is binding for purposes of challenging the language of the information postverdict. His argument, however, fails to acknowledge the more lenient standard of construction that is applied when there is a late challenge to the information. Notably, *Rosul* held that the statutory language implied knowledge of the nature of the materials under the stricter statutory interpretation standard.[1] Chambers does not cite any authority that prevents us from applying a more liberal reading to the information in this case.

In this case, the information alleged that Chambers "knowingly possessed visual or printed matter depicting a minor engaged in sexually explicit conduct . . . ." CP at 4-27. Under the liberal construction rule, the knowledge element can be fairly imputed to not only the verb but the entire direct object following the verb. "In ordinary English, where

[1] Criminal statutes are strictly construed. *State v. Larson*, 119 Wash. 123, 125, 204 P. 1041 (1922).

a transitive verb has an object, listeners in most contexts assume that an adverb (such as knowingly) that modifies the transitive verb tells the listener how the subject performed the entire action, including the object as set forth in the sentence." *Flores-Figueroa v. United States*, 556 U.S. 646, 650, 129 S. Ct. 1886, 173 L. Ed. 2d 853 (2009).

Under a more liberal construction, our Supreme Court has found a charging document sufficient even when it omits a common law element of knowledge. In *State v. Tunney*, the information failed to allege knowledge that the victim was a police officer. 129 Wn.2d 336, 339, 917 P.2d 95 (1996). Specifically, the information alleged the defendant did "'assault Officer David Shelton of the Seattle Police Department, a law enforcement officer who was performing official duties at the time of the assault.'" *Id*. at 338. The court held that under a liberal construction, the missing element could be fairly imputed from the information. *Id*. at 341. "When the crime is defined by an act and result, as in this case, the mental element relates to the result as well as the act." *Id.*; *see also State v. Hopper*, 118 Wn.2d 151, 154, 822 P.2d 775 (1992) (element of "knowingly" can be imputed from word "assault" in the information because the term "assault" implies knowing conduct); *Kjorsvik*, 117 Wn.2d at 110 (nonstatutory intent to steal element can be fairly implied from allegation that defendant "unlawfully, with force, and against the baker's will, took the money while armed with a deadly weapon").

Chambers argues that in order to be sufficient, the charging document must track the language of the to-convict jury instruction. In support of this argument, Chambers contends that the Supreme Court recently rejected the "artificial distinction between the essential elements that must be included in jury instructions and those that must be included in charging documents," citing *State v. Canela*, 199 Wn.2d 321, 332, 505 P.3d 1166 (2022). Reply Br. of Appellant at 5. We disagree that *Canela* implicitly overruled significant precedent to hold that a charging document must always contain the same language as the to-convict jury instruction. Instead, *Canela* recognized that "to-convict instructions can provide guidelines for the essential elements required in charging documents." *Id*.

The State's information mirrors the statute. Where knowledge of the nature of the materials was implied in the statute under the strict statutory interpretation standard, the language sufficiently provides notice of all essential elements under a more liberal construction. The word "knowingly" in the information modifies the acts of possession and dissemination, and the word "minor" describes the nature of the images. Chambers does not allege any prejudice from unartful language and was informed of the nature of charges and able to mount his defense.

B. INVOLVEMENT OF OUT-OF-STATE LAW ENFORCEMENT IN THE EXECUTION OF THE SEARCH WARRANT

The second issue we address in the published portion of this opinion is whether Detective Nichols was authorized to request the assistance of out-of-state law enforcement during execution of the search warrant.[2] The State responds that common law allows neighboring agencies to assist in the execution of a search warrant as subject matter experts and these outside agencies did not take over the investigation but instead took direction from Detective Nichols.

The trial court denied Chambers' motion to suppress evidence based on this theory. The trial court's unchallenged findings provide:

> Suppression hearing evidence established that Moscow Police Department Detective Eric Kjorness and two members of the Lewiston Police Department assisted in executing the search warrant at Defendant's Clarkston residence. Detective Kjorness was also involved in interviewing the Defendant at the scene and in providing technical expertise as to computer and internet issues. Defendant argues that these out-of-state officers lacked authority to be involved in the Washington search and investigation. There is no evidence of any written agreement between Washington and Idaho law enforcement agencies that would be relevant to this case.

[2] Chambers also suggests that by sitting outside his house to check access to his WiFi, Idaho Detective Birdsell was acting illegally. Opening Br. of Appellant at 61. Chambers challenged this conduct below but the court found that checking to see if nearby WiFi was secured by a password is not a search. Chambers does not assign error to this decision, nor does he posit how checking for available WiFi is illegal.

> It was Idaho police officers that initially discovered and investigated the crimes now being alleged. When they discovered that the depictions of minors engaged in sexually explicit conduct were being downloaded and shared on an IP address assigned to a Clarkston address, the case was referred to the Asotin County Sheriff's Office. From that point on, Asotin County Sheriff Detective Jackie Nichols took the lead in the Washington investigation. She obtained the search warrant and directed it [sic] execution. While she sought and obtained the presence and assistance of the Idaho officers in the search and in her investigation, Defendant cites no authority for the proposition that out-of-state officers are prohibited from providing such assistance.

CP at 251-52.

The legal issue presented is whether a Washington deputy sheriff can authorize the presence and participation of out-of-state law enforcement officers during the execution of a search warrant. As a conclusion of law set forth in an evidence suppression order, we review this legal question de novo. *State v. Rawley*, 13 Wn. App. 2d 474, 478, 466 P.3d 784 (2020).

Chambers grounds his argument in the lack of statutory authority for the Idaho officers to provide law enforcement assistance in a Washington investigation. The State contends that under common law, officers are authorized to use subject matter experts to assist in a search, even if those experts are law enforcement officers from another jurisdiction.

As the parties seem to agree, the statutes do not authorize nor do they prohibit the presence of law enforcement from other jurisdictions during a search. In certain circumstances, that do not apply here, out-of-state officers have authority to seize a person in Washington. *See* Washington Mutual Aid Peace Officer Powers Act of 1985 (chapter 10.93 RCW) and the Uniform Act on Fresh Pursuit (chapter 10.89 RCW). RCW 10.93.070 provides exceptions to the general rule that an officer's authority is restricted to his or her territorial jurisdiction. While this statute does not grant out-of-state officers the authority to act inside Washington, subsection (3) of the statute authorizes Washington peace officers to enforce the criminal laws of the state outside their territorial bounds "in response to the request of a peace officer with enforcement authority."

RCW 10.93.070(3). If the assistance is not requested, however, the presence of an officer from another jurisdiction who is tagging along for his own purposes can undermine the seizure. *State v. Bartholomew*, 56 Wn. App. 617, 622, 784 P.2d 1276 (1990).

In *Bartholomew*, Division One of this court held that a Seattle officer's presence outside his territorial jurisdiction during a warrantless felony arrest by Tacoma police could not be justified under RCW 10.93.070 where the Seattle officer was looking for evidence of a separate crime without a warrant. 56 Wn. App. at 620-25. Critically,

nothing in the record indicated that the Tacoma police needed assistance to execute a search warrant for items in the home. *Id*. at 621.

In dicta, Division One discussed situations where the presence of the Seattle officer would have been justified such as when executing a warrant where the expertise and assistance of experienced officers was requested. *Id*. at 621-22. For example, the court described participation of drug enforcement officers in executing the search of a drug manufacturing operation where safe confiscation and identification required expertise that a small rural community officer might be inadequate. *Id*. In support of that hypothetical, the court compared several federal cases analyzing 18 U.S.C. § 3105[3] to support the premise that federal officers were authorized when genuinely requested for assistance. *Id*. at 622-23; *United States v. Wright*, 667 F.2d 793 (9th Cir. 1982) (Federal Bureau of Alcohol, Tobacco, and Firearms officer executing federal search warrant properly requested state officer assistance.). The case before us presents this hypothetical.

[3] 18 U.S.C. § 3105: "A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution."

In *State v. Kern*, Division One approved the use of civilian experts to aid in the execution of a search warrant. 81 Wn. App. 308, 315, 914 P.2d 114 (1996). In *Kern*, an officer served a search warrant on a bank and instructed the bank employees to provide him with the designated records. *Id*. The bank employees participated in the record search without unnecessary supervision especially where the officer was not trained to retrieve and preserve the records in question. *Id*. The court found the delegation proper where the civilians were disinterested third parties with little possibility of exceeding the scope of the warrant. *Id*. at 316. Additionally, the court held that "[a]bsent constitutional considerations, the rules for execution and return of a warrant are essentially ministerial in nature." *Id*. at 311.

Although Chambers does not raise a constitutional argument, the United States Supreme Court has held that "it is a violation of the Fourth Amendment for police to bring . . . third parties into a home during the execution of a warrant when the presence of the third parties in the home was not in aid of the execution of the warrant." *Wilson v. Layne*, 526 U.S. 603, 614, 119 S. Ct. 1692, 143 L. Ed. 2d 818 (1999). In *Wilson*, police invited the press on a media ride-along during the execution of a warrant. The Court held that the presence of the reporters violated the defendant's Fourth Amendment rights because their "presence . . . inside the home was not related to the objectives of the

authorized intrusion." *Id*. at 611. Similar to the holding in *Bartholomew*, the Court distinguished situations where a third party "directly aided in the execution of the warrant," recognizing that such conduct "has long been approved by this Court and our common-law tradition." *Id*. at 611-12.

Here, Chambers does not dispute that Detective Kjorness was aiding Detective Nichols in the execution of the search warrant. Instead, he argues that Idaho police were "deeply involved" in the case, suggesting that they took over the search and investigation. Opening Br. of Appellant at 61. This argument is contrary to the trial court's finding that Detective Nichols was the lead investigator in this case and that she obtained the warrant and directed its execution. Chambers does not dispute this finding and there is no evidence that the Idaho officers exerted independent authority during the search. When the warrant needed to be expanded, Detective Kjorness stopped his search and Detective Nichols contacted a judicial officer to amend the warrant.

Otherwise, Chambers' argument focuses on extrajudicial issuance of warrants outside a court's jurisdiction and unauthorized arrests outside an officer's jurisdiction. Neither of these factual situations occurred here. There is no indication that the Idaho officers arrested Chambers or enforced the laws. Instead, they participated in the

execution of a search warrant at the direction of the lead investigator, Detective Nichols, and provided her with technical expertise.

For the first time on appeal, Chambers challenges the use of Idaho law enforcement experts to forensically examine the materials seized during execution of the search warrant. Chambers did not raise this challenge in his motions to suppress and did not object at the stipulated facts trial to the introduction of evidence obtained from the forensic examination by Idaho police. Citing RAP 2.5(a), the State objects to consideration of this issue because the record is undeveloped. Br. of Resp't at 66. Chambers replies that since the use of an outside agency violates his Fourth Amendment rights, the issue can be addressed as a manifest error affecting a constitutional right. RAP 2.5(a)(3).

We decline to address this issue. The exception provided in RAP 2.5(a)(3) is narrow and does not permit all asserted constitutional claims to be raised for the first time on appeal. *State v. Kirkman*, 159 Wn.2d 918, 934, 155 P.3d 125 (2007). Instead, a manifest error requires a showing of actual prejudice. *Id*. at 935. "If the trial record is insufficient to determine the merits of the constitutional claim, the error is not manifest and review is not warranted." *Id*.

Here, Chambers' attempts at showing prejudice are speculative. He contends that "[g]iven the importance that Washington courts place on strict guidelines for searches of items protected by the First Amendment and article I, section 5, one cannot assume that an officer not trained in Washington procedures would conduct the search with 'the most scrupulous exactitude.'" Opening Br. of Appellant at 67-68 (quoting *State v. Besola*, 184 Wn.2d 605, 611, 359 P.3d 799 (2015)). And yet, had Chambers raised this issue below, the facts surrounding the procedures used to forensically examine the equipment would be fully developed and part of the record. Because this issue was not preserved below and the record on appeal is insufficient, we decline to address it for the first time on appeal.

Under circumstances where the out-of-state officers were not arresting a suspect or otherwise enforcing the law, but rather acting at the direction of the lead Washington deputy to aid her in the execution of a search warrant, the presence and involvement of Detective Kjorness was not prohibited by statute and otherwise authorized by common law. The trial court properly concluded that the involvement of the Idaho officers did not require suppression of evidence.

We affirm the convictions but remand for consideration of the community custody conditions.

In the unpublished portion of the opinion, we consider challenges to the search warrant, the sufficiency of the evidence, and the community custody conditions imposed at sentencing.

A majority of the panel having determined that only the foregoing portion of this opinion will be printed in the Washington Appellate Reports and that the remainder, having no precedential value, shall be filed for public record pursuant to RCW 2.06.040, it is so ordered.

C. PROBABLE CAUSE TO SUPPORT THE SEARCH WARRANT

Chambers argues that the search warrant authorizing the search of his home lacked probable cause. He contends that the search warrant affidavit failed to establish a nexus between his computer and the IP address on the date the IP address was linked to the dissemination of depictions of minors engaged in sexually explicit conduct.

Detective Nichols from the Asotin County Sheriff's Office applied for a warrant to search Chambers' residence and electronic devices. Within her affidavit, Detective Nichols summarized that Detective Kjorness had discovered a specific IP address that was sharing images and videos of minors engaged in sexually explicit conduct and sent the information to Detective Birdsell of the Lewiston Police Department. After determining that the IP address was registered to CableOne in Lewiston, Idaho, Detective

Birdsell served CableOne with an administrative subpoena. CableOne responded with a report showing that the registered subscriber for the IP address was Michael Chambers with an address in Asotin County. Detective Nichols also averred that "Detective Birdsell went to the area near the residence. He was able to determine that access to the internet access (wifi) associated with IP address 174.126.3.13 was secured with a password." CP at 124.

Detective Nichols attached several documents to the search warrant affidavit including a police report from Detective Birdsell and the report from CableOne. Detective Nichols' affidavit did not include dates when the IP address was disseminating the illicit materials, but Detective Birdsell's report indicated that within the materials provided by Detective Kjorness, a "log showed on 10-1-2017 at 0430:56 am that IP Address 174.126.3.13" had pieces of known images of child pornography. CP at 128. Detective Birdsell's report goes on to summarize the report from CableOne as showing that the IP address "for the times 9-30-2017 to 10-1-2017" was assigned to Chambers. CP at 128.

The one-page record from CableOne indicated:

Name	MIKE CHAMBERS
Address	1865 RESERVOIR RD, CLARKSTON, WA 99403
Phone No.	(509)295-1510
Account No.	105028062
User ID	N/A
Email Address	N/A
Customer Status	Active
Creation Date	3/21/02 12:00 AM
IP Address	174.126.3.13
MAC Address	9c:3d:cf:3c:a8:8e
Lease Start	9/29/17 1:00 AM
Lease End	9/30/17 4:58 PM
Type of Service	Residential A La Carte HSD:Active 14:5B:D1:34:35:C7:HSD Service:Active

CP at 130. The CableOne record contains some ambiguous terms. Although the record indicates that the customer status is "Active" and the creation date is "3/21/02," it also includes the terms "Lease Start 9/29/17 1:00 AM" and "Lease End 9/30/17 4:58 PM." CP at 130.

An additional report by Detective Kjorness was attached to the search warrant affidavit. Detective Kjorness indicated that he continued to monitor the specific IP address 174.126.3.13 during the month of October 2017. During that time, the detective's computer made 22 additional direct connects with the suspect. During that time, "[t]he

suspect was using the BitTorrent program Vuze to access the BitTorrent network." CP at 132. On October 30, 2017, between 2146 and 2327 hours, the suspect had distributed three partial movies to the detective's computer that contained files of interest to child pornography investigations. By examining the log file generated by the detective's software, he was able to determine that a suspect at this IP address was in possession of a large number of videos suggesting they contained child pornography.

At the suppression hearing, Chambers argued that the search warrant affidavit failed to establish probable cause because the term "Lease End" must be read as indicating that Chambers' association with this IP address ended on September 30. He further argued that the search warrant affidavit did not link the IP address to the illicit materials until the next day, October 1.

The trial court denied Chambers' motion to suppress. In doing so, the court found

> It is unclear from the record provided to the issuing magistrate what was meant by the "Lease Start" and "Lease End" dates on the CableOne report. The report makes it very clear, however, that Defendant was the subscriber for "Residential A La Carte" service for this IP address, that his account was created on March 21, 2002, and that the service was active on the date the report was provided to Detective Birdsell, October 26, 2017. Detective Nichols further stated in her affidavit that after the CableOne report was received, Detective Birdsell went to the residence identified in the report, and was able to determine that there was internet access at the location for this IP address, and that access was protected by a password. It is not logical under these circumstances to construe the "Lease Start,["] "Lease End" language in the CableOne report to mean that Defendant was

> only a subscriber to the service at this IP address for 40 hours, or that he was not a subscriber on October 1, 2017.

CP at 249.

Similar to the trial court, we give great deference to a magistrate's determination of probable cause and review the issuance of a warrant for abuse of discretion. *State v. Denham*, 197 Wn.2d 759, 767, 489 P.3d 1138 (2021). The ultimate determination of probable cause is reviewed de novo. *Id*.

The United States Constitution prohibits unreasonable searches and seizures; our state constitution goes further and requires actual authority of law before the State may disturb the individual's private affairs. U.S. CONST. amend. IV; CONST. art. I, § 7. A warrant may issue only upon probable cause. *Id*. An affidavit establishes probable cause to support a search warrant if it sets forth facts sufficient to allow a reasonable person to conclude that there is a probability that the defendant is involved in specific criminal activity and that evidence of the crime can be found at the place to be searched. *Id*. In assessing the affidavit, the court is entitled to make reasonable inferences from the total facts and circumstances of the affidavit. *State v. Maddox*, 152 Wn.2d 499, 505, 98 P.3d 1199 (2004).

In order to demonstrate probable cause, the search warrant affidavit must establish "a nexus between criminal activity and the item to be seized and between that item and

the place to be searched." *State v. Neth*, 165 Wn.2d 177, 183, 196 P.3d 658 (2008). Here, the trial court found that given the other information provided in the report and affidavit, it was reasonable to infer that a computer assigned to a particular IP address on September 30 at 4:58 p.m. would have the same IP address 12 hours later on October 1 at 4:30 a.m. By the same token, the court rejected Chambers' interpretation of the term "Lease End" and found it would be illogical to assume that the terms "Lease Start" and "Lease End" meant that Chambers "was only a subscriber to the service at this IP address for 40 hours, or that he was not a subscriber on October 1, 2017." CP at 249.

These inferences are reasonable and not an abuse of discretion. *See Denham*, 197 Wn.2d at 770 (judge did not abuse her discretion in making reasonable inferences to find a nexus between defendant's cell phone location and evidence of a burglary). While it is not clear that the CableOne report connected Chambers' computer to the IP address on October 1, it is reasonable to infer that this nexus existed on September 30 at 4:58 p.m. It is also reasonable, given the information provided in the CableOne report and the search warrant affidavit, to infer that Chambers' internet connection had the same IP address 12 hours later. As the court noted, Chambers' account had been active for a considerable time and was noted as still active in the report. Detective Kjorness also provided consistency by indicating that throughout the entire month of October, his computer

continued to connect with the same IP address, using the same BitTorrent program to access the BitTorrent network.

Nor was the finding of probable cause legal error. Probable cause, as the name implies, concerns probabilities, not certainties. *Denham*, 197 Wn.2d at 769. It is determined from the totality of facts set before the judge in the affidavit and is based on commonsense conclusions. *Id*. In support of his argument on probable cause, Chambers makes several arguments that we decline to address on appeal, either because he fails to assign error to the trial court's decision, or he failed to make the argument below sufficient for the court to determine relevant facts.

First, Chambers suggests in his briefing that Detective Nichols made two false statements in her affidavit.[4] He argues that the second "misrepresentation violated

[4] Chambers contends that Detective Nichols makes a false statement in her affidavit when she claims that the CableOne report indicates that the IP address was assigned to Chambers' computer on October 1. Opening Br. of Appellant at 40. Chambers also contends that this statement is false: "'Detective Birdsell went to the area near the residence [and] was able to determine that access to the internet access (wifi) associated with IP address 174.126.3.13 was secured with a password.'" Opening Br. of Appellant at 39.

Franks."[5] Opening Br. of Appellant at 49.

Chambers did not preserve a *Franks* issue on appeal. Prior to trial, Chambers made the same claim of false statements and moved for a *Franks* hearing. The trial court denied his request, concluding that any misrepresentations were not intentional or in reckless disregard for the truth. Chambers then filed a second motion to suppress, arguing that the search warrant affidavit failed to establish probable cause. The trial court denied this motion in a separate opinion.

While Chambers assigns error to the court's denial of his second motion to suppress, he did not assign error to the court's decision to deny a *Franks* hearing. RAP 10.3. Nor does he clearly set out that the trial court erred in denying his request for a *Franks* hearing. Instead, in his reply brief, Chambers argues that the *Franks* issue is a "subsidiary issue[ ]" of his probable cause argument. Reply Br. of Appellant at 18-19. He fails to cite any authority for this argument, therefore, we assume that none exists and decline to consider his argument. *DeHeer v. Seattle Post-Intelligencer*, 60 Wn.2d 122,

[5] At the defendant's request, the court must hold a *Franks* hearing if the defendant makes a preliminary showing that the affiant included a false statement knowingly and intentionally, or with reckless disregard for the truth, and the false statement was necessary to a finding of probable cause. *Franks v. Delaware*, 438 U.S. 154, 155-56, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978).

126, 372 P.2d 193 (1962); RAP 10.3(a)(6); *Cowiche Canyon Conservancy v. Bosley*, 118 Wn.2d 801, 809, 828 P.2d 549 (1992).

Next, Chambers argues that even if the last connection between his computer and the IP address was at 4:58 p.m. on September 30, this connection was almost instantly stale because the search warrant affidavit fails to indicate whether the IP address is static or dynamic. Chambers failed to make this argument below as a basis for challenging probable cause. Had he done so, the trial court would have entered findings of fact and conclusions of law on the issue of staleness. CrR 3.6(b). Findings are especially important when considering factual issues. Whether information is stale for purposes of probable cause is a factual determination. *Maddox*, 152 Wn.2d at 505-06 (In determining whether information is stale, the court looks to the totality of circumstances and applies a commonsense approach.). Generally, we will not consider issues raised for the first time on appeal. *State v. Kirkman*, 159 Wn.2d 918, 926, 155 P.3d 125 (2007); RAP 2.5(a).

Even if we were to consider the staleness issue, however, we would conclude that the magistrate did not abuse her discretion in determining that the information contained in the search warrant affidavit was not stale. Chambers argues that the difference of one day made the information stale. In reality, the difference was at most 12 hours. In addition, Detective Kjorness' report indicates that consistent information continued to be

exchanged with the same IP address for the entire month of October, suggesting that even if this was a dynamic IP address, it did not change on a frequent or daily basis. It was reasonable to infer that an IP address assigned to Chambers' computer at 4:58 p.m. on September 30 was not stale at 4:30 a.m. on October 1.

The magistrate judge did not abuse her discretion in finding a sufficient nexus existed between the IP address associated with child pornography and Chambers' computers. Nor did the magistrate err in concluding there was probable cause to issue a search warrant.

D. PARTICULARITY AND BREADTH OF THE WARRANT

Next, Chambers contends that even if the warrant was supported by probable cause, the warrant nonetheless violates the Fourth Amendment's requirement for particularity and is overbroad. Our review of this issue is de novo. *State v. Perrone*, 119 Wn.2d 538, 549, 834 P.2d 611 (1992).

After finding probable cause that Chambers was dealing in depictions of minors engaged in sexually explicit conduct, the superior court issued a search warrant for his person and home in Asotin County, Washington. The introductory paragraph of the warrant indicates that there is probable cause to believe four crimes have been committed and that evidence of these crimes is concealed on or within certain property. The warrant

identifies the crimes as dealing, sending, viewing, and possessing "depictions of minor[s] engaged in sexually explicit conduct" and recites the applicable statutes. CP at 136. The warrant authorized law enforcement to "Seize and Forensically Search and Examine, if located, the following: Any evidence of the aforementioned crimes including but not limited to:" and then lists 14 items. CP at 137.

Item 1 authorized law enforcement to search for evidence of the aforementioned crimes including "[a]ny digital or physical image or movie containing or displaying depictions of a minor engaged in sexually explicit conduct." CP at 137 (boldface omitted). Below this first item, the warrant sets forth verbatim statutory definitions of numerous terms such as "internet session," "photograph," "[v]isual or printed matter," "[s]exually explicit conduct," "[m]inor," and "[l]ive performance." CP at 137-38.

Items 2 through 7, as well as items 9 through 11 authorize the search and seizure of devices and equipment including computers, computer networks and systems, computer programs and software, digital storage media, cell or mobile phones, cameras, printers, portable digital devices and peripheral computer equipment.

Item 8 specifies "[a]ny developed film, slides, or printed photographs, which include evidence of depictions of minors engaged in sexually explicit conduct as well as images of possible child victims." CP at 139 (boldface omitted).

Items 12 through 14 include the search for items showing identity, ownership, or control of the devices.

Chambers argues that the warrant was overbroad because it did not explicitly limit the search of devices in items 2 through 14 for evidence related to the crimes involving minors engaged in sexually explicit conduct as specifically defined in item 1. Opening Br. of Appellant at 53. We disagree.

A warrant based on probable cause must specifically describe the places to be searched and the items to be seized. U.S. CONST. amend. IV; *State v. Besola*, 184 Wn.2d 605, 609, 359 P.3d 799 (2015). The requirement for specificity includes particularity and breadth. *State v. McKee*, 3 Wn. App. 2d 11, 22, 413 P.3d 1049 (2018), *rev'd on other grounds*, 193 Wn.2d 271, 438 P.3d 528 (2019). "'"Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based."'" *Id*. at 23 (quoting *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993) (quoting *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 856-57 (9th Cir. 1991))).

The degree of specificity required in describing and identifying the items to be seized and searched varies according to the circumstances and the type of items involved. *Id*. at 23-24. When the items to be seized and searched implicate materials protected by

the First Amendment, the court must apply "'scrupulous exactitude'" to the Fourth Amendment's particularity requirement. *Perrone*, 119 Wn.2d at 550. But even under this stricter standard, warrants are tested and interpreted in a commonsense, practical manner, rather than in a hypertechnical sense. *Id*. at 549.

A warrant is overbroad if its description of contraband encompasses materials that are lawful to possess, such as adult pornography. *Besola*, 184 Wn.2d at 610. In *Besola*, the court found that the "Search Warrant Provisions Related to Print Materials" was overbroad. *Id*. at 611 (emphasis omitted). Although the warrant identified the crimes being investigated, the warrant authorized the search of printed pornographic materials and photographs, "but particularly of minors." *Id*. at 608-09. While the warrant listed the statutory definition of the crime, the warrant did not use this definition to describe the materials being sought. *Id*. at 614. As the court noted, if the citation to the statute was intended as a limitation on the materials to be seized, then it would have been unnecessary to include the modifier "but particularly of minors" when describing the photographs to be seized. *Id*. at 615. Instead, the items could have been described with more particularity by simply using the precise statutory language to describe the materials being sought. *Id*. at 610.

A search warrant authorizing the seizure and search of nonprint materials, such as computers and cell phones can also be overbroad, although the degree of specificity in describing these items is different. As *Besola* implied, print materials are different.[6] Print materials can be seen and immediately identified as evidence of a crime. Therefore, an officer searching a home can look at print material and seize it if it is relevant or leave it if it is not.

On the other hand, items stored on digital devices are not immediately identifiable and searching them for evidence usually requires someone with forensic equipment and special skills.

> If a magistrate reasonably finds it probable that an individual has engaged in criminal dealings with child pornography and that digital 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.

State v. Friedrich, 4 Wn. App. 2d 945, 963, 425 P.3d 518 (2018). Although it is reasonable to allow computers and digital storage devices to be seized, as *Friedrich*

[6] Although the warrant in *Besola* also authorized the seizure and search of equipment such as computer and memory storage devices, the court's overbreadth decision was specifically limited to the print materials identified in the warrant. *Besola*, 184 Wn.2d at 611.

suggests, the subsequent forensic search of these items must still be limited to looking for evidence of the crimes.

In *McKee*, the warrant indicated there was probable cause to believe the defendant had committed the crimes of dealing and possession of depictions of minors engaged in sexually explicit conduct and authorized police to seize his cell phone without limitation. 3 Wn. App. 2d at 29. While the warrant cited the criminal statutes being investigated, similar to *Besola*, the language of the statute was not used to limit the description of the data sought from the cell phone. Instead of limiting the search of the phone to depictions of minors engaged in sexually explicit conduct, the warrant authorized police to look through text messages, call logs, and calendars "without regard to whether the data is connected to the crime." *McKee*, 3 Wn. App. 2d at 29.

In *State v. Vance*, Division Two considered the constitutionality of a warrant authorizing the seizure of digital storage equipment upon probable cause that the defendant was possessing and dealing in depictions of minors engaged in sexually explicit conduct. 9 Wn. App. 2d 357, 444 P.3d 1214 (2019). The warrant included citation to the criminal statutes being investigated and then described the electronic devices to be seized including a list of devices and media "'capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of evidence, contraband,

fruits, or instrumentalities of such crimes.'" *Id*. at 361. Upon seizure, the warrant authorized the items to be transferred to the Cybercrime Unit "'for the examination . . . of data . . . to include: graphic/image files[,] . . . emails, spreadsheets, databases . . . that are related to the production, creation, collection, trade, sale, distribution, or retention of files depicting minors engaged in sexually explicit acts/child pornography.'" *Id*. (emphasis omitted).

The court found the warrant to be valid and not overbroad. Not only did the warrant explain that there was probable cause to search for the identified crimes, but the electronic items to be seized were limited to devices capable of committing or storing evidence of the crimes. *Id*. at 365-66. Finally, the forensic search was limited to particular types of data that were specifically related to the crimes as described. *Id*. at 366. While the court recognized that it would have been helpful had the warrant included the statutory definition of "sexually explicit conduct," the regular references within the warrant to crimes being investigated limited the property that officers could seize. *Id*.

In this case, the warrant specifically cites the statutes and identifies the crimes being investigated. The warrant goes on to authorize the seizure of any evidence of the identified crimes including item 1: "Any digital or physical image or movie containing or displaying depictions of a minor engaged in sexually explicit conduct." CP at 137

(boldface omitted). Following this description are the statutory definition of every relevant term, including "'[s]exually explicit conduct.'" CP at 137. The warrant then goes on to list electronic devices to be seized including computers, cell phones, software, and storage media. CP at 138-39.

Unlike the warrants in *Besola*, *McKee*, and *Vance*, the warrant here uses specific statutory terms and then provides the statutory definitions for these terms. By using these well-defined terms, the warrant limits the search of items seized to data specifically connected to the crime.

Chambers argues that the warrant found valid in *Vance* is distinguishable from the warrant in this case. Specifically, Chambers contends that items 2 through 14 are listed without specific limitation or reference back to the particularized description in item 1. While we agree that a specific reference back to item 1 would have provided even more exactitude, we conclude that the warrant, taken as a whole, makes it clear that the search of items 2 through 14 is limited to "[a]ny digital or physical image or movie containing or displaying depictions of a minor engaged in sexually explicit conduct" as listed in item 1. CP at 137.

Borrowing from the logic applied in *Besola*, Chambers also argues that if the limitations set out in item 1 were meant to apply to items 2 through 14, then it would be

unnecessary for item 8 to modify the search of "developed film, slides, or printed photographs," to "evidence of depictions of minors in sexually explicit conduct as well as images of possible child victims." CP at 139 (boldface omitted). This analogy fails because, as we noted above, print material is different. Item 8 in this search warrant identified print material that is immediately recognizable as illegal. Unlike electronic equipment that must be seized and then searched offsite, print material that does not depict minors engaged in sexually explicit conduct is not unlawful to possess and should not be seized.

Contrary to Chambers' hypertechnical argument, a commonsense reading of the warrant in this case identified equipment that probably contained evidence of the crimes and then limits the forensic search of this equipment to evidence of the crimes listed in the warrant as specifically defined in the first item. *See Besola*, 184 Wn.2d at 615 ("Even where the constitution requires scrupulous exactitude, '[s]earch warrants are to be tested and interpreted in a commonsense, practical manner, rather than in a hypertechnical sense.'") (quoting *Perrone,* 119 Wn.2d at 549) (alteration in original)).

E. SUFFICIENCY OF THE EVIDENCE FOR COUNTS 1, 2, AND 3

In the next issue, Chambers argues that the facts are insufficient to support convictions for three counts of dealing in depictions of child pornography, two counts in

the first degree and one count in the second degree (counts 1, 2, and 3). Specifically, he contends that making images available on a peer-to-peer network does not constitute publishing, disseminating, or exchanging said images. Instead, Chambers argues that the detective in this case essentially reached into his computer and took the files. He contends that the stipulated facts do not demonstrate that he knew these files were available for sharing. Finally, Chambers argues that his shared network contained partial files that cannot be definitively said to contain sexually explicit images of minors despite their matching "hash" to identified child pornography electronic files.

The parties in this case waived a jury trial and stipulated to the admission of police reports as evidence.[7] Following a bench trial, appellate review is limited to determining whether substantial evidence supports the findings of fact and, if so, whether the findings support the conclusions of law. *State v. Homan*, 181 Wn.2d 102, 105-06, 330 P.3d 182 (2014). We review challenges to a trial court's conclusions of law de novo. *Id*. at 106. Substantial evidence is evidence sufficient to persuade a fair-minded person of the truth of the asserted premise. *Id.*

[7] In lieu of a trial brief, the State presented the court with jury instructions, and the trial court filled in jury verdict forms instead of entering findings of fact and conclusions of law as required by CrR 6.1(d). We do not condone this procedure.

Evidence is sufficient to support a guilty verdict if any rational trier of fact, viewing the evidence and inferences from it in the light most favorable to the State, could find the elements of the charged crime beyond a reasonable doubt. *State v. Salinas*, 119 Wn.2d 192, 201, 829 P.2d 1068 (1992). When a defendant challenges the sufficiency of the evidence, he or she admits the truth of all of the State's evidence. *Id.* Credibility determinations are for the trier of fact and are not subject to review. *State v. Camarillo*, 115 Wn.2d 60, 71, 794 P.2d 850 (1990), *abrogated on other grounds by State v. Crossguns*, 199 Wn.2d 282, 291, 505 P.3d 529 (2022). The court must defer to the trier of fact on issues of conflicting testimony, credibility of witnesses, and the persuasiveness of the evidence. *State v. Thomas*, 150 Wn.2d 821, 875, 83 P.3d 970 (2004), *abrogated in part on other grounds by Crawford v. Washington*, 541 U.S. 36, 124 S. Ct. 1354, 158 L. Ed. 2d 177 (2004). In determining the sufficiency of the evidence, we do not consider circumstantial evidence any less reliable than direct evidence. *State v. Delmarter*, 94 Wn.2d 634, 638, 618 P.2d 99 (1980).

We first consider whether storing images or videos on a shared directory on a peer-to-peer network is sufficient to support a conviction for dealing in depictions of child pornography. For purposes of this issue, the State was required to prove that Chambers knowingly "published, disseminated, or exchanged" three visual or printed images or

videos of child pornography.[8] RP at 219; RCW 9.68A.050. Chambers argues that these verbs require active behavior as opposed to passive behavior. He makes no attempt to argue statutory interpretation, fails to suggest any definitions for these three verbs to support his argument, and fails to provide any supporting authority.

We find his argument unpersuasive. The plain, ordinary meaning of the word "publish," includes "to disseminate to the public." MERRIAM-WEBSTER ONLINE DICTIONARY (available at https://www.merriam-webster.com/dictionary/publish (last visited Sept. 29, 2022). The evidence presented to the trial court indicated that the program used by Chambers required the user to make files on their own computers available to others. In other words, the user must take an affirmative step to make material available for sharing. This is legally sufficient to support a finding that Chambers published the illicit images and videos.

Under similar federal statutes, federal courts have repeatedly determined that making files available in a shared directory is sufficient to support a conviction for dealing in child pornography. *See United States v. Budziak*, 697 F.3d 1105, 1109 (9th Cir. 2012) (evidence sufficient to find defendant distributed digital files by maintaining

[8] The only difference between first and second degree charges is the nature of the matter depicted which is not an issue in this case.

them in a shared folder accessible to other users of his LimeWire software, despite his assertion that he disabled the sharing function on the software); *United States v. Shaffer*, 472 F.3d 1219, 1223-24 (10th Cir. 2007) ("distribution" in the federal child pornography statute included defendant's allowance of third parties access to his computer files for download regardless of whether or not he actively "pushed" files to other users of the file sharing software).

Despite evidence that the images and videos on Chambers' computer had been made available for sharing on a peer-to-peer network, Chambers argues there is insufficient evidence that he knowingly disseminated these files. Instead, he argues that the evidence presented to the court shows that he did not realize or believe that his files were available for sharing and that he was not good at computers. The State responds that while it is true that Chambers said these things, the court did not have to believe Chambers. Instead, there was sufficient competing evidence for the court to find that Chambers' exculpatory statements to law enforcement were not credible. Both parties point to Chambers' comment that he thought he had the "'outgoing totally shut down.'" CP at 38.

The parties stipulated to the evidence presented to the court and indicated as part of the stipulation that the evidence submitted was "an accurate record of [the] facts."

CP at 259. The evidence reflects testimony supporting both the State's charges and Chambers' defenses. Although the facts were stipulated, as the fact finder, the judge weighed any disputed evidence and engaged in credibility determinations. A bench trial on stipulated facts is still a trial. *State v. Mierz*, 127 Wn.2d 460, 468, 901 P.2d 286 (1995). By stipulation, the parties agree that what the State presents is what the witnesses would say. *State v. Johnson*, 104 Wn.2d 338, 342-43, 705 P.2d 773 (1985). However, the State must still prove the charges beyond a reasonable doubt and the defendant is not precluded from offering contrary evidence. *Id*.

Here the trial court weighed the evidence and ultimately rejected Chambers' exculpatory explanations for his use of peer-to-peer software and his claim of ignorant accidental configuration. Chambers' comment demonstrates that he knew how to shut down outgoing files so that they were not sharable. It is reasonable to infer that he knew how to make them shareable. Taken in the light most favorable to the State, there is sufficient evidence that Chambers intended to make the files shareable. The BitTorrent program requires a user to actively designate files to be available for upload by others, and the detective was able to upload files from Chambers' computer. Intent can be inferred from the software setting and the availability of the files for distribution.

Chambers also suggests that the evidence was insufficient because Detective Kjorness was only able to download a partial file from Chambers' computer. This argument fails because Chambers stipulated that the contents of each exhibit was sufficient to find him guilty.

F. COMMUNITY CUSTODY CONDITIONS

In his final issue on appeal, Chambers challenges two of the community custody conditions imposed as part of his sentence. Chambers was convicted of using his computer to possess and disseminate depictions of minors engaged in sexually explicit conduct. Within the judgment and sentence, the trial court included numerous restrictions and requirements including treatment. The court also required that Chambers "[s]ubmit to and pay for any polygraph examination, as directed by his Supervising Officer or the sexual deviancy treatment provider." CP at 356. The court limited his ability to access the internet: "No access or use of the internet or any device which has the ability to access the internet without specific written permission from his Supervising Officer." CP at 356.

Chambers challenges these two provisions asserting that they are both constitutionally overbroad in violation of his First Amendment rights. The State concedes his right to relief in the case of the internet access restriction and requests remand for the trial court to narrow the language.

Generally, community custody conditions are reviewed for an abuse of discretion. *State v. Padilla*, 190 Wn.2d 672, 677, 416 P.3d 712 (2018). Where Chambers failed to object to community custody conditions at the trial court level, it must first be determined whether his challenge involves manifest constitutional error. Appellate courts may consider claims of manifest constitutional error raised for the first time on appeal provided that an adequate record exists to consider the claim. RAP 2.5(a); *State v. McFarland*, 127 Wn.2d 322, 333, 899 P.2d 1251 (1995). "[F]or an objection to a community custody condition to be entitled to review for the first time on appeal, (1) it must be manifest constitutional error or a sentencing condition that . . . is 'illegal or erroneous' as a matter of law and (2) it must be ripe. If it is ineligible for review for one reason, we need not consider the other." *State v. Peters*, 10 Wn. App. 2d 574, 583, 455 P.3d 141 (2019).[9] A raised issue is ripe if it is primarily legal, does not require further factual development, and the challenged action is final. *State v. Cates*, 183 Wn.2d 531, 534, 354 P.3d 832 (2015). Imposition of an unconstitutional community custody

[9] Chambers primarily challenges the broadness of the conditions, but for the first time in his reply he appears to assert a vagueness challenge as to the future actions of his probation officer that would be unripe. Reply Br. of Appellant at 34; *Cowiche Canyon Conservancy*, 118 Wn.2d at 809 ("An issue raised and argued for the first time in a reply brief is too late to warrant consideration.").

condition is manifestly unreasonable. *State v. Valencia*, 169 Wn.2d 782, 792, 239 P.3d 1059 (2010).

Discretionary community custody conditions must comply with statutory requirements and not excessively burden a defendant's constitutional rights. *State v. Johnson*, 197 Wn.2d 740, 746-49, 487 P.3d 893 (2021). A judge abuses their discretion in imposing community custody conditions in violation of the legal parameters set by RCW 9.94A.703. *State v. Geyer*, 19 Wn. App. 2d 321, 326, 496 P.3d 322 (2021). Only after statutory and constitutional requirements are met does the abuse of discretion standard require deference to the trial court. *Id.*

The complete prohibition of Chambers' use of the internet without prior permission of his community corrections supervisor is similar to restrictions found overbroad in *Geyer*. In that case, this court held that restricting the use of any computer or electronic device capable of connecting to the internet without prior permission was unnecessarily broad and impermissibly burdened his freedom of speech. *Id*. at 329; U.S. CONST. amend. I; WASH. CONST. art. I, § 5. For this reason, we accept the State's concession and agree that this provision is overbroad.

We deny Chambers' challenge to the polygraph condition. On a number of occasions, Washington courts have previously found polygraph testing constitutional.

Polygraph testing may be utilized to monitor compliance with the requirement of making reasonable progress in treatment or with other special conditions of community supervision. *State v. Combs*, 102 Wn. App. 949, 952, 10 P.3d 1101 (2000) (citing *State v. Riles*, 135 Wn.2d 326, 342-43, 957 P.2d 655 (1998), *abrogated on other grounds by Valencia*, 169 Wn.2d at 792-93.). Chambers' challenge is not so much focused on the polygraph testing itself but his interpretation of the word "any" in the condition phrase "Submit to and pay for any polygraph examination . . . ." CP at 356. Much like the defendants in both the *Combs* and *Riles* cases, he is concerned with limitation of the purpose and subject matter of the examinations.

In *Combs*, the trial court ordered unlimited polygraph testing in order to monitor James Combs' compliance with his other conditions of community placement. 102 Wn. App. at 952. This court concluded "that the language of Mr. Combs's judgment and sentence, taken as a whole, impliedly limits the scope of polygraph testing to monitor only his compliance with the community placement order and not as a fishing expedition to discover evidence of other crimes, past or present." *Id*. at 952-53. To arrive at this holding, the court discussed and found persuasive the Division One holding in *Riles* that "although the challenged portion of the community placement order did not expressly limit the scope of the polygraph testing, a sufficient limitation was implicitly imposed,

considering the context of the entire order." *Id*. at 952 (citing *State v. Riles*, 86 Wn. App. 10, 16-17, 936 P.2d 11 (1997), *aff'd*, 135 Wn.2d 326.

Likewise, in this case, given the language used and the conditions imposed including treatment, we can infer that the polygraph testing is to be limited to monitoring compliance. The polygraph condition is not an abuse of discretion and not a manifest constitutional error. If the community custody officer subjects Chambers to improper questioning during a later polygraph examination, Chambers may challenge at that time when such issue is ripe. *State v. Vant*, 145 Wn. App. 592, 603, 186 P.3d 1149 (2008).

We accept the State's concession, strike the internet restriction from the community custody conditions, and remand so that the trial court can consider a modified restriction. While the polygraph condition language implies a limitation to community custody purposes, since we are remanding for the court to consider internet conditions, it may be appropriate for the trial court to explicitly clarify the polygraph on remand.

We affirm the convictions but remand for reconsideration of the community custody conditions.

Staab, J.

WE CONCUR:

Lawrence-Berrey, A.C.J.

Fearing, J.