

FILED
Court of Appeals
Division II
State of Washington
2/21/2020 11:12 AM
NO. 53362-6-II

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

STATE OF WASHINGTON, Respondent

v.

JORDEN DAVID KNIGHT, Appellant

FROM THE SUPERIOR COURT FOR CLARK COUNTY
CLARK COUNTY SUPERIOR COURT CAUSE NO.17-1-00568-1

BRIEF OF RESPONDENT

Attorneys for Respondent:

ANTHONY F. GOLIK
Prosecuting Attorney
Clark County, Washington

AARON T. BARTLETT, WSBA #39710
Deputy Prosecuting Attorney

Clark County Prosecuting Attorney
1013 Franklin Street
PO Box 5000
Vancouver WA 98666-5000
Telephone (564) 397-2261

TABLE OF CONTENTS

RESPONSE TO ASSIGNMENTS OF ERROR.....	1
I. Knight waived his new argument that Vancouver police unlawfully searched his Dropbox files. Nonetheless, Knight’s Dropbox files were lawfully obtained by all the relevant entities and the derivative evidence was properly admitted against him at trial.....	1
II. The community custody conditions about which Knight complains—prohibiting certain “romantic relationships” without approval and requiring urine and breath testing for alcohol—are unconstitutionally vague and not crime-related, respectively. These two conditions should be amended in such a way to make them lawful or stricken from Knight’s judgment and sentence.	1
STATEMENT OF THE CASE.....	1
A. Procedural History.....	1
B. Statement of Facts	2
1. Background Facts.....	2
2. Knight Investigation.....	5
ARGUMENT.....	7
I. Knight waived his new argument that Vancouver police unlawfully searched his Dropbox files. Nonetheless, Knight’s Dropbox files were lawfully obtained by all the relevant entities and the derivative evidence was properly admitted against him at trial.....	7
1. <i>Knight’s new arguments are waived</i>	8
2. <i>The Vancouver Police Department lawfully searched Knight’s Dropbox files provided to it by NCMEC.</i>	11
a) Standard of Review	11
b) The Vancouver Police did not disturb Knight’s private affairs	12
<i>There is no privacy interest in contraband</i>	13
<i>There is no privacy interest in items made publicly available.</i>	14
<i>There is no privacy interest in digital files that violate a service provider’s terms of service.</i>	15

II.	Even if Knight had a privacy interest in the contraband he publicly shared in violation of Dropbox’s TOS, the Vancouver police still lawfully opened three of Knight’s files provided to it by NCMEC.....	19
	<i>Private searches vs. the private search doctrine</i>	19
	<i>The Silver Platter Doctrine</i>	21
III.	Probable Cause Existed to Support the Issuance of the Warrants Even Absent the Descriptions of the Depictions.....	24
	<i>The independent source doctrine</i>	25
IV.	The community custody conditions about which Knight complains—prohibiting certain “romantic relationships” without approval and requiring urine and breath testing for alcohol—are unconstitutionally vague and not crime-related, respectively. These two conditions should be amended in such a way to make them lawful or stricken from Knight’s judgment and sentence.	28
	CONCLUSION.....	28

TABLE OF AUTHORITIES

Cases

<i>California v. Ciraolo</i> , 476 U.S. 207, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986).....	12, 13
<i>Franks v. Delaware</i> , 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978)	25
<i>In re Teddington</i> , 116 Wn.2d 761, 808 P.2d 156 (1991).....	21, 24
<i>Katz v. U.S.</i> , 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).....	12
<i>One 1958 Plymouth Sedan v. Pennsylvania</i> , 380 U.S. 693, 85 S.Ct. 1246, 14 L.Ed.2d 170 (1965).....	13
<i>State v. Alaway</i> , 64 Wn.App. 796, 828 P.2d 591 (1992).....	13
<i>State v. Bertrand</i> , 165 Wn.App. 393, 267 P.3d 511 (2011).....	11
<i>State v. Betancourth</i> , 190 Wn.2d 357, 413 P.3d 566 (2018).....	25, 26, 27
<i>State v. Bradley</i> , 105 Wn.2d 898, 719 P.2d 546 (1986).....	21, 23
<i>State v. Brelvis Consulting LLC</i> , 7 Wn.App.2d 207, 436 P.3d 818 (2018)	13
<i>State v. Carter</i> , 151 Wn.2d 118, 85 P.3d 887 (2004).....	14
<i>State v. Chenoweth</i> , 160 Wn.2d 454, 158 P.3d 595 (2007).....	25, 27
<i>State v. Clark</i> , 48 Wn.App. 850, 743 P.2d 822 (1987).....	19
<i>State v. Coates</i> , 107 Wn.2d 882, 735 P.2d 64 (1987).....	26
<i>State v. Courcy</i> , 48 Wn.App. 326, 739 P.2d 98 (1987).....	14
<i>State v. Eisfeldt</i> , 163 Wn.2d 628, 185 P.3d 580 (2008).....	19, 20
<i>State v. Friedrich</i> , 4 Wn.App.2d 945, 425 P.3d 518 (2018).....	3
<i>State v. Gaines</i> , 154 Wn.2d 711, 116 P.3d 993 (2005).....	25, 26
<i>State v. Garbaccio</i> , 151 Wn.App. 716, 214 P.3d 168 (2009).....	9
<i>State v. Garrison</i> , 118 Wn.2d 870, 827 P.2d 1388 (1992).....	25
<i>State v. Garvin</i> , 166 Wn.2d 242, 207 P.3d 1266 (2009).....	11, 12
<i>State v. Gordon</i> , 172 Wn.2d 671, 260 P.3d 884 (2011).....	10
<i>State v. Grimes</i> , 165 Wn.App. 172, 267 P.3d 454 (2011).....	10
<i>State v. Hamilton</i> , 179 Wn.App. 870, 320 P.3d 142 (2014).....	9
<i>State v. Hayes</i> , 165 Wn.App. 507, 265 P.3d 982 (2011).....	8, 10
<i>State v. Higgs</i> , 177 Wn.App. 414, 311 P.3d 1266 (2014).....	9
<i>State v. Hill</i> , 123 Wn.2d 641, 870 P.2d 313 (1994).....	12
<i>State v. Huft</i> , 106 Wn.2d 206, 720 P.2d 838 (1986).....	25
<i>State v. Kirkman</i> , 159 Wn.2d 918, 155 P.3d 125 (2007).....	9
<i>State v. Knight</i> , 176 Wn.App. 936, 309 P.3d 776 (2013).....	11
<i>State v. Lazcano</i> , 188 Wn.App. 338, 354 P.3d 233 (2015).....	9
<i>State v. Lindsey</i> , 177 Wn.App. 233, 311 P.3d 61 (2013).....	10
<i>State v. Martinez</i> , 2 Wn.App.2d 55, 408 P.3d 721 (2018).....	21, 22, 24

<i>State v. McFarland</i> , 127 Wn.2d 322, 899 P.2d 1251 (1995).....	10
<i>State v. Mezquia</i> , 129 Wn.App. 118, 118 P.3d 378 (2005)	21
<i>State v. Miles</i> , 160 Wn.2d 236, 156 P.3d 864 (2007)	13
<i>State v. O'Hara</i> , 167 Wn.2d 91, 217 P.3d 756 (2009).....	10
<i>State v. Peppin</i> , 186 Wn.App. 901, 347 P.3d 906, 910–12 (2015).....	14, 18
<i>State v. Ramirez</i> , 5 Wn.App.2d 118, 425 P.3d 534 (2018).....	10
<i>State v. Reeder</i> , 184 Wn.2d 805, 365 P.3d 1243 (2015).....	12, 13
<i>State v. Scott</i> , 110 Wn.2d 682, 757 P.2d 492 (1998).....	8
<i>State v. Strine</i> , 176 Wn.2d 742, 293 P.3d 1177 (2013).....	9
<i>State v. Thein</i> , 138 Wn.2d 133, 140, 977 P.2d 582 (1999).....	24
<i>State v. Valdez</i> , 167 Wn.2d 761, 224 P.3d 751 (2009)	12
<i>State v. Walter</i> , 66 Wn.App. 862, 833 P.2d 440 (1992)	19
<i>State v. Wilson</i> , 108 Wn.App. 774, 31 P.3d 43 (2001).....	9
<i>State v. Young</i> , 135 Wn.2d 498, 957 P.2d 681 (1998).....	13
<i>U.S. v. Ackerman</i> , 296 F.Supp.3d 1267, 1273 (D. Kan. 2017)....	13, 15, 16, 17, 18
<i>U.S. v. Ackerman</i> , 831 F.3d 1292, 1295-1300 (10th Cir. 2016) ...	20, 23, 27
<i>U.S. v. Coyne</i> , 387 F.Supp.3d 387, 395-96 (D. Vt. 2018)	16
<i>U.S. v. DiTomasso</i> , 56 F.Supp.3d 584, 597 (S.D. N.Y 2014).....	16
<i>U.S. v. Ganoe</i> , 538 F.3d 1117, 1127 (9th Cir. 2008).....	15
<i>U.S. v. Jacobsen</i> , 466 U.S. 109, 104, S.Ct. 1652, 80 L.Ed.2d 85 (1984) .	14
<i>U.S. v. Jones</i> , 31 F.3d 1304, 1311 (4th Cir. 1994).....	14
<i>U.S. v. Maclin</i> , 393, F.Supp.3d 701, 705 (2019)	2, 15
<i>U.S. v. Perrine</i> , 518 F.3d 1196, 1204-05 (10th Cir. 2008)	15
<i>U.S. v. R.V.</i> , 157 F.Supp.3d 207, 231 (E.D. N.Y. 2016).....	15
<i>U.S. v. Sawyer</i> , 786 F. Supp. 2d 1352, 1356 (N.D. Ohio 2011)	15
<i>U.S. v. Stratton</i> , 229 F.Supp.3d 1230, 1241-42 (D. Kan. 2017).....	16
<i>U.S. v. Stults</i> , 575 F.3d 834, 842-43 (8th Cir. 2009).....	15

Other Authorities

18 U.S.C. § 2258A.....	3
Ben Adams, <i>What Is Fourth Amendment Contraband?</i> , 69 Stan. L. Rev. 1137, 1160-62 (2017).....	14
https://www.dropbox.com/terms#acceptable_use	4, 18

Rules

CrR 3.6.....	1
RAP 2.5.....	10
RAP 2.5(a)	8, 10
RAP 2.5(a)(3).....	8, 10

Constitutional Provisions

U.S. CONST, Fourth Amendment..... 8, 12, 19, 20, 21, 23, 24
WA CONST, Article I § 7 8, 12, 15, 18, 19, 20

RESPONSE TO ASSIGNMENTS OF ERROR

- I. **Knight waived his new argument that Vancouver police unlawfully searched his Dropbox files. Nonetheless, Knight's Dropbox files were lawfully obtained by all the relevant entities and the derivative evidence was properly admitted against him at trial.**
- II. **The community custody conditions about which Knight complains—prohibiting certain “romantic relationships” without approval and requiring urine and breath testing for alcohol—are unconstitutionally vague and not crime-related, respectively. These two conditions should be amended in such a way to make them lawful or stricken from Knight's judgment and sentence.**

STATEMENT OF THE CASE

A. PROCEDURAL HISTORY

Jorden David Knight was charged by second amended information with five counts of Possession of Depictions of a Minor Engaged in Sexually Explicit Conduct in the First Degree occurring on or about or between March 21, 2016 and March 23, 2017. CP 685-87.

Prior to trial, Knight filed six CrR 3.6 motions to suppress evidence and two motions to reconsider particular motions to suppress following their denial. CP 172-78, 197-202, 223-229, 258-262, 315-18, 465-68, 593-95, 633-37. All but one of these motions was denied and no substantive evidence was ultimately suppressed. CP 499-528, 690-93, 699-702.

The case proceeded to a bench trial before the Honorable Gregory Gonzales, which commenced on April 1, 2019 and concluded the next day with the court's verdict finding Knight guilty as charged. CP 837-850; RP 145-333. The trial court sentenced Knight to a standard range sentence of 77 months of total confinement. CP 869, 871; RP 370. Knight filed a timely notice of appeal. CP 887.

B. STATEMENT OF FACTS

This case began when Dropbox, Inc. submitted a CyberTip that one of its users, Jorden Knight, was utilizing its service to store 322 files depicting minors engaged in sexually explicit conduct. CP 2.

1. Background Facts

Dropbox is a file hosting service operated by Dropbox, Inc. that offers cloud storage, file synchronization, and client software. *U.S. v. Maclin*, 393, F.Supp.3d 701, 705 n. 2 (2019). Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. *Id.* Files placed in this folder also are accessible through a website and mobile phone applications. *Id.*

Additionally, when Dropbox:

users upload files to their Dropbox accounts, they can choose whether to keep files private within their accounts, to share files with specified Dropbox users, or to share files with the public by creating a ‘shared link.’ Files that are shared with the public can be accessed over the Internet by any person who knows the Uniform Resource Locator (‘URL’) for the shared link.

A Dropbox user who creates a shared link for a file can then share that file by distributing the URL for the shared link. Any member of the public who clicks that link or who otherwise accesses the shared link’s URL can view the associated file without logging into a Dropbox account.

CP 479.

Dropbox is required by federal law¹ to submit “CyberTips” to the National Center for Missing and Exploited Children (“NCMEC”) CyberTipline if it discovers depictions of minors engaged in sexually explicit conduct stored on its servers. CP 478. Dropbox has created specific procedures to comply with the law including “manually review[ing]” each image of suspected “child pornography” “by a member of the content safety team before it is reported to NCMEC” and disabling “the [user’s] account, which renders the reported content inaccessible.” CP 478.

¹ “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. *State v. Friedrich*, 4 Wn.App.2d 945, 949, 425 P.3d 518 (2018) (quoting 18 U.S.C. § 2258A.

When Dropbox sends a CyberTip to NCMEC the company indicates whether each particular file was “reviewed” and whether it was “publicly available.” CP 356-422, 478-79. If the file is marked as reviewed, the image or file was looked at, and confirmed to be alleged “child pornography,” by a human reviewer as described above. CP 478. If the file is marked as publicly available, that means that the user created a “shared link,” which allows the file to be “accessed over the Internet by any person who knows the [URL] for the shared link” or with whom the link was shared “without logging into a Dropbox account.” RP 479.

Dropbox also has terms of service², acceptable use policies³, and privacy policies that regulate the manner in which its users can utilize Dropbox and alert its users about what information of theirs can and will be disseminated. CP 430-438. For example, the company’s privacy policy warns its users under a “Law & Order” heading that it may “may disclose your information” if “such disclosure is reasonably necessary to [] comply with the law.” CP 437.

² The “Dropbox Terms of Service” explicitly informs the user that by “using our Services, you’re agreeing to be bound by these Terms, our Privacy Policy and Acceptable Use Policy.” CP 431.

³ https://www.dropbox.com/terms#acceptable_use

2. Knight Investigation

Jorden Knight had a Dropbox account. CP 2-3, 6, 366. On March 23, 2016, Dropbox submitted a CyberTip to NCMEC that indicated that one of its users had uploaded 322 files that were suspected depictions of minors engaged in sexually explicit conduct, and, as part of the CyberTip, submitted the files and Knight's account information. CP 356-422. Each of the suspected depictions was reviewed by a human at Dropbox and "publicly available." CP 367-416. Upon receiving the CyberTip, NCMEC reviewed two of the image files and "found what appears to be CHILD PORNOGRAPHY." CP 418. NCMEC also developed additional information linking Knight to the Dropbox account. CP 418-420. Next, NCMEC forwarded the CyberTip to the Seattle Internet Crimes against Child taskforce, which in turn assigned the case to the Vancouver Police Digital Evidence Cybercrime Unit. CP 2, 41-42, 422.

A Vancouver police detective accessed the provided 322 files, viewed three of them, and concluded that these files (videos) appeared to be depictions of minors engaged in sexually explicit conduct. CP 2-3, 42-44. A slew of search warrants followed. These warrants were sent to Dropbox, Comcast, and Google, and eventually served on Knight's residence and his cellphone. CP 5, 38-50, 203-218, 230-246, 263-310. The police located five images of children engaged in sexually explicit conduct

on Knight's cellphone in the unallocated space. RP 173-74, 189, 192, 204-05, 211-18.⁴ Similarly, the police also discovered evidence of a "social-media app" called Kik on which Knight engaged in discussions with other users about sharing and trading—utilizing his Dropbox account—depictions of minors engaged in sexual conduct. RP 223-27, 230-38, 240-255, 259-268; Ex. 16, 18-32.

The State presented the above depictions found on Knight's phone as evidence at the bench trial. Additionally, one of Knight's roommates during the relevant time period testified that no other person at the residence accessed Knight's room or used his electronics (cellphone or computer). RP 178-181. This fact was corroborated by Knight himself. RP 167. Knight did not testify.

///

///

///

///

///

///

⁴ The particular five images admitted into evidence corresponded to the charged counts, but the police found significantly more than five such images on Knight's cellphone and also discovered videos of minor children engaged in sexual activity,. *See, e.g.* RP 169-170, 218-222, 229-30.

ARGUMENT

I. Knight waived his new argument that Vancouver police unlawfully searched his Dropbox files. Nonetheless, Knight's Dropbox files were lawfully obtained by all the relevant entities and the derivative evidence was properly admitted against him at trial.

Prior to trial, Knight filed six motions to suppress evidence and two motions to reconsider particular motions to suppress following their denial. CP 172-78, 197-202, 223-229, 258-262, 315-18, 465-68, 593-95, 633-37. These motions challenged the lawfulness of Dropbox's initial discovery of the 322 depictions that Knight stored on its servers, NCMEC's review of two of Knight's files (depictions) provided to it by Dropbox, the search warrants served on Comcast, Google, and Dropbox, the search warrants that authorized a search of Knight's residences and electronic devices, and a warrant that authorized GPS monitoring of Knight's vehicle. CP 172-78, 197-202, 223-229, 258-262, 315-18, 465-68, 593-95, 633-37; *See* RP 1-131.

Knight, however, did not make the argument that he makes now: that the "Vancouver Police illegally searched Mr. Knight's Dropbox files without a warrant." *Compare* Brief of Appellant at 7-16 *with* CP 172-78, 197-202, 223-229, 258-262, 315-18, 465-68, 593-95, 633-37; RP 1-131. Knight also makes a new argument regarding the "silver platter doctrine" by abandoning his claim below that the doctrine did not apply because of

an “agency” relationship between NCMEC and the Vancouver Police Department and now arguing that it does not apply where NCMEC, a governmental entity, does “not conduct a federal investigation” regardless of whether the evidence was lawfully obtained under the Fourth Amendment.⁵ Compare CP 594-95; RP 104 with Br. of App. at 16-17.

Knight did not present these arguments to the trial court. Nor does Knight raise issue preservation or brief and argue RAP 2.5(a)(3) to explain why he should be able to raise these arguments for the first time on appeal. As a result, this Court should consider the arguments waived and not consider them.

1. *Knight’s new arguments are waived*

The general rule is that an issue, theory, or argument not presented at trial will not be considered on appeal. RAP 2.5(a); *State v. Hayes*, 165 Wn.App. 507, 514, 265 P.3d 982 (2011) (citation omitted). This “rule reflects a policy of encouraging the efficient use of judicial resources.” *State v. Scott*, 110 Wn.2d 682, 685, 757 P.2d 492 (1998) (citation omitted). Our courts “will not sanction a party’s failure to point out at trial an error which the trial court, if given the opportunity, might have been able to correct to avoid an appeal and a consequent new trial.” *Scott*,

⁵ To be more specific, the contention is that evidence lawfully obtained by NCMEC under the Fourth Amendment that does not also comport with article I, section 7 of the Washington Constitution cannot be turned over to Washington police agencies under the silver platter doctrine. Br. of App. at 14-17.

110 Wn.2d at 685 (citation omitted). The theory of issue preservation by timely objection also “facilitates appellate review by ensuring that a complete record of the issues will be available, and prevents adversarial unfairness by ensuring that the prevailing party is not deprived of victory by claimed errors that he had no opportunity to address.” *State v. Lazcano*, 188 Wn.App. 338, 356, 354 P.3d 233 (2015) (citing *State v. Strine*, 176 Wn.2d 742, 749-50, 293 P.3d 1177 (2013)).

And while a party need not intone magic words in order to preserve an argument for appeal, a party does need to at least make the essential argument and the “argument should be more than fleeting.” *Id.* at 355; *State v. Wilson*, 108 Wn.App. 774, 778, 31 P.3d 43 (2001). This rule also applies to suppression motions as, “[e]ven if a defendant objects to the introduction of evidence at trial, he or she ‘may assign evidentiary error on appeal only on a specific ground made at trial.’” *State v. Hamilton*, 179 Wn.App. 870, 878, 320 P.3d 142 (2014) (quoting *State v. Kirkman*, 159 Wn.2d 918, 926, 155 P.3d 125 (2007)); *State v. Higgs*, 177 Wn.App. 414, 423-24, 311 P.3d 1266 (2014); *State v. Garbaccio*, 151 Wn.App. 716, 731, 214 P.3d 168 (2009) (holding that because defendant’s “present contention was not raised in his suppression motion, and because he did not seek a ruling on this issue from the trial court, we will not consider it for the first time on appeal”).

An exception to this rule exists, however, for manifest errors affecting a defendant's constitutional rights. RAP 2.5(a)(3); *Hayes*, 165 Wn.App. at 514. "In order to benefit from this exception, 'the [defendant] must identify a constitutional error and show how the alleged error actually affected the [defendant]'s rights at trial.'" *State v. Grimes*, 165 Wn.App. 172, 180, 267 P.3d 454 (2011) (alterations in original) (quoting *State v. Gordon*, 172 Wn.2d 671, 676, 260 P.3d 884 (2011)) (quoting *State v. O'Hara*, 167 Wn.2d 91, 98, 217 P.3d 756 (2009)). The "manifest error" standard is exacting: "[t]he record must contain 'nearly explicit' facts demonstrating a constitutional violation." *State v. Ramirez*, 5 Wn.App.2d 118, 132-33, 425 P.3d 534 (2018) (citation omitted). Accordingly, "[i]f the facts necessary to adjudicate the claimed error are not in the record on appeal, no actual prejudice is shown and the error is not manifest." *State v. McFarland*, 127 Wn.2d 322, 899 P.2d 1251 (1995). Furthermore, in order to show actual prejudice regarding a suppression issue, the defendant "must show the trial court likely would have granted the motion if made." *Id.* at 333-34.

More than that, however, is required; in order to take advantage of one of the RAP 2.5(a) exceptions on appeal, a defendant must actually present a RAP 2.5 argument to this Court and bears the burden of proving an exception exists. *State v. Lindsey*, 177 Wn.App. 233, 247, 311 P.3d 61

(2013); *State v. Knight*, 176 Wn.App. 936, 951, 309 P.3d 776 (2013);
State v. Bertrand, 165 Wn.App. 393, 400-03, 267 P.3d 511 (2011).

Here, as noted above, Knight's argument that the "Vancouver Police illegally searched Mr. Knight's Dropbox files without a warrant" was not argued to the trial court. And Knight fails to present this Court with an argument as to why he can raise the propriety of this search for the first time on appeal. Moreover, as discussed below, because Knight's new claims are without merit he cannot show that the trial court would have granted a motion based on his new arguments had he made them to that court. Consequently, Knight's new arguments are waived.

2. *The Vancouver Police Department lawfully searched Knight's Dropbox files provided to it by NCMEC.*

Even assuming Knight preserved his new arguments or may raise them for the first time on appeal, his arguments fail because the police lawfully searched his Dropbox files.

a) Standard of Review

When a defendant challenges a trial court's denial of a suppression motion, "an appellate court determines whether substantial evidence supports the challenged findings of fact and whether the findings support the conclusions of law." *State v. Garvin*, 166 Wn.2d 242, 249, 207 P.3d

1266 (2009). Findings of fact are verities on appeal when unchallenged⁶ or provided that “there is substantial evidence to support the findings.” *State v. Hill*, 123 Wn.2d 641, 644, 870 P.2d 313 (1994); *State v. Valdez*, 167 Wn.2d 761, 767, 224 P.3d 751 (2009). “Substantial evidence exists where there is a sufficient quantity of evidence in the record to persuade a fair-minded, rational person of the truth of the finding.” *Id.* A trial court’s conclusions of law following a suppression hearing are reviewed de novo. *Garvin*, 166 Wn.2d at 249.

b) The Vancouver Police did not disturb Knight’s private affairs

A Fourth Amendment search does not occur unless “the individual manifested a subjective expectation of privacy in the object of the challenged search” and “society [is] willing to recognize that expectation as reasonable.” *California v. Ciraolo*, 476 U.S. 207, 211, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) (citing *Katz v. U.S.*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)). Article I, section 7, our constitutional analog, protects “those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass.” *State v. Reeder*, 184 Wn.2d 805, 814, 365 P.3d 1243 (2015) (citations and internal quotation omitted). The corollary of which is that “[i]f a private affair is not

⁶ Knight does not assign error to any findings of fact entered by the trial court. Br. of App. at 2.

disturbed, then there is no violation of article I, section 7.” *Id.* (citing *State v. Miles*, 160 Wn.2d 236, 244, 156 P.3d 864 (2007)).⁷

Moreover, a defendant has the “burden of proving a disturbance of his [or her] private affairs under article I, section 7.” *State v. Young*, 135 Wn.2d 498, 510, 957 P.2d 681 (1998). To determine whether a privacy interest—a particular expectation of privacy that a citizen should be entitled to hold—exists under our constitution courts look to “what kind of protection has been historically afforded to the interest asserted” and to “the nature and extent of the information that may be obtained as a result of government conduct.” *Reeder*, 184 Wn.2d at 814; *State v. Brelvis Consulting LLC*, 7 Wn.App.2d 207, 229, 436 P.3d 818 (2018).

There is no privacy interest in contraband

“Contraband” is defined as an “object, the possession of which, without more, constitutes a crime.” *State v. Alaway*, 64 Wn.App. 796, 799, 828 P.2d 591 (1992) (quoting *One 1958 Plymouth Sedan v. Pennsylvania*, 380 U.S. 693, 699, 85 S.Ct. 1246, 1250, 14 L.Ed.2d 170 (1965)). Because of its inherently criminal character, courts have consistently held that a citizen is not entitled to hold an expectation of privacy in contraband. *State v. Carter*, 151 Wn.2d 118, 126-27, 85 P.3d

⁷ Similarly, if a person does not have a reasonable expectation of privacy “in the object of the challenged search” there is no violation of the Fourth Amendment. *Ciraolo*, 476 U.S. at 211; *U.S. v. Ackerman*, 296 F.Supp.3d 1267, 1273 (D. Kan. 2017) (*Ackerman II*).

887 (2004) (holding that a defendant could not claim “his private affairs were disturbed when he voluntarily placed the gun on a table in open view [and] . . . [t]he contraband nature of the gun was immediately apparent. . . .”); *State v. Courcy*, 48 Wn.App. 326, 332, 739 P.2d 98 (1987); *U.S. v. Jones*, 31 F.3d 1304, 1311 (4th Cir. 1994); *U.S. v. Jacobsen*, 466 U.S. 109, 123, 123 n. 23, 104, S.Ct. 1652, 80 L.Ed.2d 85 (1984); Ben Adams, *What Is Fourth Amendment Contraband?*, 69 Stan. L. Rev. 1137, 1160-62 (2017). “Child pornography,” certain controlled substances, and certain weapons are the paradigmatic examples of contraband where “possession is only lawful for government actors or specifically authorized organizations, meaning that there is no chance an individual will ever have a legitimate expectation of privacy in those materials—either possession is lawful (in which case it is not private) or possession is private (in which case it is not lawful). Adams, *supra*, at 1160-62, 1165.

There is no privacy interest in items made publicly available.

Our courts have long denied “article I, section 7 protections to information voluntarily held out to the public.” *State v. Peppin*, 186 Wn.App. 901, 910, 347 P.3d 906, 910–12 (2015). Unsurprisingly then, courts have “consistently held that a person who installs and uses file sharing software does not have a reasonable expectation of privacy in the files to be shared on his or her computer.” *Id.* at 908-910 (citing *U.S. v.*

Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008); *U.S. v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008); *U.S. v. Stults*, 575 F.3d 834, 842-43 (8th Cir. 2009)). Washington is in accord, acknowledging that the “inherent nature of peer to peer software is the *public* sharing of digital computer files” and that “[i]ndividuals using file sharing software cannot expect a privacy interest in files they hold open to the public,” a public that includes law enforcement. *Id.* at 910 (emphasis added).

This principle extends to those who use file sharing software, but limit access to his or her files to “friends” or other smaller groups. *Maclin*, 393 F. Supp.3d at 711 (N.D. Ohio 2019); *U.S. v. Sawyer*, 786 F. Supp. 2d 1352, 1356 (N.D. Ohio 2011). Moreover, as previously noted, Dropbox is software that allows for peer to peer file sharing and allows its users to make their files stored on Dropbox “publicly available.” CP 479; *Maclin*, 393 F.3d at 702 n.2, 711; *U.S. v. R.V.*, 157 F.Supp.3d 207, 231 (E.D. N.Y. 2016).

There is no privacy interest in digital files that violate a service provider’s terms of service.

A person who uses an internet or electronic service provider for internet access, email services, or cloud storage must agree to that provider’s terms of service. *Ackerman II*, 296 F. Supp.3d at 1272-73. Generally, a provider’s terms of service (“TOS”), which include

acceptable use policies, inform a user that he or she may not use the provider's services to engage in unlawful activities, that their usage of the service may be monitored, and that any unlawful activity may be reported to the police. *Id.* (citations omitted). The existence "of a TOS agreement diminishes a user's objectively reasonable expectation of privacy" in the user's activities on the service provider's services and the files that are hosted by the service provider. *Id.*; *U.S. v. Stratton*, 229 F.Supp.3d 1230, 1241-42 (D. Kan. 2017); *see also U.S. v. DiTomasso*, 56 F.Supp.3d 584, 597 (S.D. N.Y. 2014) (holding that the existence of a service provider's TOS functions as waiver of "Fourth Amendment rights"); *contra U.S. v. Coyne*, 387 F.Supp.3d 387, 395-96 (D. Vt. 2018).

Ackerman II is instructive. 296 F.Supp.3d 1267. There, the defendant utilized AOL as his internet service provider, which included email service. *Id.* At some time during the defendant's use of the service, AOL detected an email sent from him that had four attached images one of which it (AOL) identified as child pornography. *Id.* at 1270-71. As a result of this discovery, AOL terminated the defendant's account and submitted a CyberTip to NCMEC with the flagged email and the four image files. *Id.* at 1271. The defendant challenged the subsequent search⁸ by NCMEC and

⁸ The search in this case was the opening of the image files and review of the email.

argued that he retained a reasonable expectation of privacy in his email and images attached to it. *Id.*

Ackerman II did not agree and held that the defendant did not have an objectively reasonable expectation of privacy due to the existence of AOL's terms of service. *Id.* at 1273. Notably, AOL's TOS informed the defendant that:

he could not participate in illegal activities. AOL's TOS also informed Defendant that if he participated in illegal activities or did not comply with AOL's TOS, it could take technical, legal, or other actions without notice to him.

Id. at 1272. Accordingly, the court concluded that the defendant could not "establish a reasonably objective expectation of privacy in this particular email and its four attachments (containing child pornography) after AOL terminated his account for violating its TOS." *Id.* And because he did not have a reasonable expectation of privacy in those files, NCMEC did not conduct an unlawful search when it reviewed the defendant's email and opened the attached image files. *Id.* at 1273.

Here, Knight used Dropbox⁹, and violated its TOS and acceptable use policies, to *publicly share contraband* (depictions of minors engaged in sexually explicit conduct). CP 367-416, 479. Thus, from the onset Knight did not have a “privacy interest in [the] files” under article I section 7. *Peppin*, 186 Wn.App. at 910. To the extent that any privacy interest remained in the files, it was extinguished by Dropbox’s human review confirming that each and every file was contraband and NCMEC’s more limited confirmatory review. CP 356, 367-416, 418, 478-79. Accordingly, Knight did not have a valid privacy interest in the files by the time they were in the possession of the Vancouver police department and, as a result, the opening of the three files to view them did not constitute a search under the Washington Constitution. And just like the defendant in *Ackerman II*, Knight cannot be heard to complain about later “searches” of such files since he had no expectation of privacy in them. Knight’s new argument fails.

⁹ Knight created a Dropbox account and used its services, and, thus, had to agree and abide by its terms of service, acceptable use policies, and privacy policies. CP 430-38. These terms and policies regulated the manner in which Knight could utilize Dropbox and informed him what information of his could and would be disseminated. CP 430-438. For example, the company’s privacy policy alerted Knight under a “Law & Order” heading that it may “may disclose your information” if “such disclosure is reasonably necessary to [] comply with the law.” CP 437. Similarly, Dropbox’s acceptable use policy prohibits its users from “publish[ing] or shar[ing] materials that are unlawfully pornographic or indecent.” https://www.dropbox.com/terms#acceptable_use.

II. Even if Knight had a privacy interest in the contraband he publicly shared in violation of Dropbox’s TOS, the Vancouver police still lawfully opened three of Knight’s files provided to it by NCMEC.

Private searches vs. the private search doctrine

Neither the Fourth Amendment nor article I section 7 provide protection from “private searches” or require the “exclusion of evidence obtained from private citizens acting on their own initiative.” *State v. Clark*, 48 Wn.App. 850, 855, 743 P.2d 822 (1987) (citations omitted); *State v. Walter*, 66 Wn.App. 862, 867, 833 P.2d 440 (1992). In other words, “citizens do not retain a privacy interest in evidence of a crime obtained by a private actor and delivered to the police.” *State v. Eisfeldt*, 163 Wn.2d 628, 638 n. 9, 185 P.3d 580 (2008) (internal quotation omitted).

In contrast, the “private search doctrine” recognized under the Fourth Amendment is “inapplicable under article I, section 7 of the Washington Constitution.” *Id.* “Under the private search doctrine a warrantless search by the police does not offend the Fourth Amendment if the search does not expand the scope of the private search.” *Id.* at 636. For example, if a private actor searched a suspect’s backpack and found drugs and then brought the backpack to the police, the police could search the backpack and seize the drugs without a warrant provided they did not

expand the scope of the private actor's search. This is not true under article I, section 7, and so the police officer's search of the backpack would be unconstitutional and the drug evidence suppressed. *Id.* at 638. But on the other hand, and as explained above, "constitutional protections do not apply" if that same private actor removed the drugs from the backpack and delivered them to the police, i.e., the drug evidence would be admissible against the owner of the backpack. *Id.* at 638 n. 9.

Here, the private search doctrine applies to NCMEC's review of two of Knight's 322 files sent by Dropbox as part of the CyberTip since it is a federal governmental entity to which the Fourth Amendment applies. *See U.S. v. Ackerman*, 831 F.3d 1292, 1295-1300 (10th Cir. 2016) ("*Ackerman I*"). As previously discussed, Dropbox, a private actor, had a human review each and every file included as part of its CyberTip by viewing them. This was the private search. Consequently, when NCMEC performed a confirmatory review of only two of the provided files its search did not "expand the scope of the private search" performed by Dropbox. *Eisfeldt*, 163 Wn.2d at 636; *Ackerman I*, 831 F.3d at 1305-08. Thus, the private search doctrine applies and NCMEC's search of Knight's files was lawful under the Fourth Amendment. And by virtue of the Dropbox's private search and the private search doctrine applying to NCMEC's subsequent search, by the time Knight's files had been

transferred to the Vancouver police both “searches” of Knight’s files, which confirmed them to be “child pornography,” were lawful.

The Silver Platter Doctrine

The general rule is that “evidence lawfully obtained under federal standards by [federal] . . . officials is admissible in state court even if the search and seizure would have violated state law.” *State v. Bradley*, 105 Wn.2d 898, 902-03, 719 P.2d 546 (1986); *In re Teddington*, 116 Wn.2d 761, 772-75, 808 P.2d 156 (1991). This is known as the “silver platter doctrine” and it has two elements that must be met in order for evidence obtained in a foreign jurisdiction to be admissible in Washington: “(1) the foreign jurisdiction lawfully obtained evidence; and (2) the [Washington] officers did not act as agents or cooperate or assist the foreign jurisdiction.” *State v. Mezquia*, 129 Wn.App. 118, 132–33, 118 P.3d 378 (2005) (citation omitted); *State v. Martinez*, 2 Wn.App.2d 55, 64-65, 408 P.3d 721 (2018). A necessary corollary to the silver platter doctrine is that said lawfully obtained evidence “may be transferred to state authorities for use in a Washington State criminal proceeding” without the need for a warrant. *Teddington*, 116 Wn.2d at 772-75.

Martinez is instructive. 2 Wn.App.2d 55. There, Texas police lawfully seized, searched, and made a mirror image of the defendant’s computer’s hard drive. *Id.* at 62-63. The Texas police then sent the mirror

image of the hard drive, along with “two actual laptop computers” to the WSP in Washington who searched the mirror image hard drive without a warrant. *Id. Martinez* held that the silver platter doctrine applied since “(1) the search was lawful in Texas and (2) the Washington officers did not act as agents for Texas or cooperate with or assist Texas in any way” and that, as a result, the *warrantless* search was lawful. *Id.* at 64-65.

Here, Knight advances a new argument that the silver platter doctrine does not apply because NCMEC, despite being “a government entity for the purposes of the Fourth Amendment,” did “not conduct a federal investigation in this case.” Br. of App. at 16-17. But no legal authority is provided for the proposition that first element of the silver platter doctrine test (“the foreign jurisdiction lawfully obtained evidence”) in any way depends on whether the foreign jurisdiction or officials conduct an investigation. Br. of App. at 17. And the argument that NCMEC is a governmental entity for the purposes of the Fourth Amendment, which Knight advanced at length below, but not for silver platter doctrine cannot be reconciled. CP 201, 465-68, 594-95; Br. of App. at 16-17. In fact, Knight does not even attempt to offer a principle by which to distinguish the two positions. Br. of App. at 16-17.

Indeed, the reasons why courts have found NCMEC to be a governmental entity for the purposes of the Fourth Amendment directly

refute Knight's claim for why the silver platter doctrine should not apply to NCMEC's acceptance and review of files. *See Ackerman I*, 831 F.3d at 1295-1304. For example, as *Ackerman I* explained "NCMEC's law enforcement powers extend well beyond those enjoyed by private citizens" and its "two primary authorizing statutes . . . mandate its collaboration with federal (as well as state and local) law enforcement in over a dozen different ways, many of which involve duties and powers conferred on and enjoyed by NCMEC but no other private person." *Id.* at 1296. Similarly, "NCMEC's CyberTipline functions . . . illustrate[] and confirm[] the special law enforcement duties and powers it enjoys." *Id.* Furthermore, "[l]aw enforcement agents participate at varying levels in its daily operations, . . . government officials enjoy a sizeable presence on its board[, and] [a]s much as 75 percent of its budget . . . comes from the federal government." *Id.* at 1298 (footnotes omitted).

In short, NCMEC acts like any other branch of the federal government with some law enforcement powers; if it violates the Fourth Amendment the evidence it discovers is suppressed and if its search is lawful under the Fourth Amendment the evidence it discovers may be lawfully provided to Washington authorities under the silver platter doctrine. *Id.* at 1308-09; *Bradley*, 105 Wn.2d at 902-03 (holding that evidence seized by United States Customs officials admissible under the

silver platter doctrine); *Teddington*, 116 Wn.2d at 773, 775. And here NCMEC—in a manner seemingly similar to an investigation—received Knight’s files from Dropbox, reviewed two of the files confirming them to be “CHILD PORNOGRAPHY,” developed additional information linking Knight to the Dropbox account, and determined that the account user was based in Washington and in Vancouver specifically. CP 418-420. NCMEC accomplished all of this lawfully under the Fourth Amendment and then ultimately transferred the information and files to the Vancouver police department, though NCMEC did not act as agents of the VPD or vice versa. Thus, the silver platter doctrine applies and the Vancouver police lawfully opened and viewed three of Knight’s Dropbox files. *Cf. Martinez*, 2 Wn.App.2d at 62-65.

III. Probable Cause Existed to Support the Issuance of the Warrants Even Absent the Descriptions of the Depictions.

“Probable cause exists if the affidavit in support of the warrant sets forth facts and circumstances sufficient to establish a reasonable inference” that evidence of the crime can be found at the place to be searched. *State v. Thein*, 138 Wn.2d 133, 140, 977 P.2d 582 (1999). In fact, probable cause itself “may be based on hearsay, a confidential informant’s tip, and other unscrutinized evidence that would be

inadmissible at trial.” *State v. Chenoweth*, 160 Wn.2d 454, 475, 158 P.3d 595 (2007) (citing *State v. Huft*, 106 Wn.2d 206, 209-210, 720 P.2d 838 (1986)); *Franks v. Delaware*, 438 U.S. 154, 164-65, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978). That these types of evidence can establish probable cause is unsurprising since “the concept of probable cause . . . requires not certainty but only sufficient facts and circumstances to justify a reasonable belief that evidence of criminal activity will be found.” *Id.* (citation omitted).

The independent source doctrine

Under the independent source doctrine, evidence tainted by “unlawful police action is not subject to exclusion ‘provided that it ultimately is obtained pursuant to a valid warrant or other lawful means independent of the unlawful action.’” *State v. Betancourth*, 190 Wn.2d 357, 364-65, 413 P.3d 566 (2018) (quoting *State v. Gaines*, 154 Wn.2d 711, 718, 116 P.3d 993 (2005)). “The independent source doctrine recognizes that probable cause may exist for a warrant based on legally obtained evidence when the tainted evidence is suppressed.” *Id.* at 365. Therefore, reviewing courts are to uphold a search warrant unless the illegally obtained information in the search warrant affidavit was “*necessary* to the finding of probable cause.” *State v. Garrison*, 118 Wn.2d 870, 874, 827 P.2d 1388 (1992) (emphasis in original) (citations

omitted); *State v. Coates*, 107 Wn.2d 882, 887-89, 735 P.2d 64 (1987).

The independent source doctrine ensures that the State neither benefits from its unlawful conduct nor is it placed in a worse position than it otherwise would have occupied. *Gaines*, 154 Wn.2d at 720; *Betancourth*, 190 Wn.2d at 365, 371-72.

Our Supreme Court recently described the independent source doctrine in *Betancourth*:

In its classic form, the independent source doctrine applies when the State procures the challenged evidence pursuant to a valid warrant, untainted by prior illegality. In the first type of independent source scenario, police conduct an initial unwarranted search of a constitutionally protected area, during which they discover but do not seize incriminating items. Police later obtain a search warrant for the area and seize the evidence during the warranted search.

For example, in *Gaines*, the police performed an illegal warrantless search of the trunk of the defendant's car, during which officers saw what appeared to be the barrel of an assault rifle and numerous rounds of ammunition. Rather than seizing the items, officers immediately closed the trunk without disturbing the contents. The following day, the police sought a search warrant for the defendant's trunk, which included a single reference to the officer's observation of the weapon, as well as other evidence to establish probable cause. After obtaining the warrant and searching the vehicle, the police recovered the rifle and ammunition from the trunk of the defendant's car. We concluded that this conduct violated article I, section 7 and that the appropriate remedy was to strike all references to the initial illegal search from the warrant affidavit when assessing whether probable cause existed to issue the original warrant; we held that the evidence was ultimately seized pursuant to a lawful warrant.

190 Wn.2d at 368-69 (internal citations omitted).

Here, probable cause existed for the issuance of the warrants even assuming that the Vancouver police performed an unlawful search of three of the files provided by NCMEC. When striking out the descriptions of images viewed from the warrant affidavit the magistrate was still left with the information from the CyberTip that “Dropbox reported that 322 files suspected of containing child pornography were uploaded to a Dropbox account,” that NCMEC “[s]taff reviewed the files uploaded and they appeared to contain child pornography,” and the information that linked Jordan Knight to the Dropbox account associated with the files mentioned in the CyberTip reported to NCMEC. CP 179-188, 203-215, 230-242, 263-302.¹⁰ Given the reliability of the tip and the manner in which the files were identified as prohibited material, the remaining information in the affidavit was more than enough “to justify a reasonable belief that evidence of criminal activity will be found.” CP 68-75; *Chenoweth*, 160 Wn.2d at 475. As even *Ackerman I* noted “we are confident that NCMEC’s law enforcement partners will struggle not at all to obtain warrants to open emails when the facts in hand suggest, as they surely did here, that a crime against a child has taken place.” 831 F.3d at 1309.

¹⁰ Additionally, evidence received in executing the first warrants, e.g. Dropbox, resulted in additional incriminating information that was included in the search warrant affidavit for Knight’s residences. CP 294-95.

IV. The community custody conditions about which Knight complains—prohibiting certain “romantic relationships” without approval and requiring urine and breath testing for alcohol—are unconstitutionally vague and not crime-related, respectively. These two conditions should be amended in such a way to make them lawful or stricken from Knight’s judgment and sentence.

The State agrees with Knight’s analysis of his community custody conditions. New and controlling case law supports Knight’s position on the “romantic relationship” condition and no evidence was presented in the trial court that Knight consumed alcohol or that alcohol was in any way related to his crimes. Consequently, these two conditions should be amended in such a way to make them lawful or stricken from Knight’s judgment and sentence.

CONCLUSION

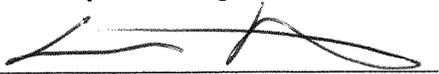
For the reasons argued above, Knight’s convictions should be affirmed and the complained about conditions amended or stricken.

DATED this 21st day of February, 2020.

Respectfully submitted:

ANTHONY F. GOLIK
Prosecuting Attorney
Clark County, Washington

By:


AARON T. BARTLETT, WSBA #39710
Deputy Prosecuting Attorney
OID# 91127

CLARK COUNTY PROSECUTING ATTORNEY

February 21, 2020 - 11:12 AM

Transmittal Information

Filed with Court: Court of Appeals Division II
Appellate Court Case Number: 53362-6
Appellate Court Case Title: State of Washington, Respondent v Jorden David Knight, Appellant
Superior Court Case Number: 17-1-00568-1

The following documents have been uploaded:

- 533626_Briefs_20200221111127D2875198_5072.pdf
This File Contains:
Briefs - Respondents
The Original File Name was Brief - Respondent.pdf

A copy of the uploaded files will be sent to:

- stephanie@newbrylaw.com

Comments:

Sender Name: Ashley Smith - Email: ashley.smith@clark.wa.gov

Filing on Behalf of: Aaron Bartlett - Email: aaron.bartlett@clark.wa.gov (Alternate Email:
CntyPA.GeneralDelivery@clark.wa.gov)

Address:
PO Box 5000
Vancouver, WA, 98666-5000
Phone: (564) 397-5686

Note: The Filing Id is 20200221111127D2875198