

FILED  
Court of Appeals  
Division I  
State of Washington  
2/18/2021 2:52 PM

FILED  
SUPREME COURT  
STATE OF WASHINGTON  
2/18/2021  
BY SUSAN L. CARLSON  
CLERK

99515-0

Supreme Court No. (to be set)  
Court of Appeals No. 81837-6-I

---

**IN THE SUPREME COURT  
OF THE STATE OF WASHINGTON**

---

STATE OF WASHINGTON,

Respondent,

v.

JORDEN D. KNIGHT,

Appellant.

---

PETITION FOR REVIEW  
BY THE APPELLANT, JORDEN D. KNIGHT

---

ON APPEAL FROM THE SUPERIOR COURT OF THE  
STATE OF WASHINGTON FOR CLARK COUNTY  
THE HONORABLE GREGORY M. GONZALES, JUDGE

---

STEPHANIE TAPLIN  
Attorney for Appellant  
Newbry Law Office  
623 Dwight St.  
Port Orchard, WA 98366  
(360) 876-5567

## TABLE OF CONTENTS

I.	IDENTITY OF PETITIONER.....	1
II.	COURT OF APPEALS DECISION.....	1
III.	ISSUES PRESENTED FOR REVIEW .....	1
IV.	STATEMENT OF THE CASE.....	1
V.	ARGUMENT WHY REVIEW SHOULD BE ACCEPTED.....	4
	A. Mr. Knight Preserved his Challenge to the Warrantless Search Conducted by Vancouver Police in this Case. ....	6
	B. The Warrantless Search by Vancouver Police Violated Mr. Knight’s Constitutional Right to Privacy.....	6
	1. The Washington Constitution broadly protects privacy interests. ....	7
	2. Mr. Knight’s Dropbox files were protected by article I, section 7 of the Washington Constitution.....	10
	3. The “silver platter doctrine” does not apply in this case.....	16
VI.	CONCLUSION.....	19

## TABLE OF AUTHORITIES

### Cases

<i>Illinois v. Rodriguez</i> , 497 U.S. 177, 110 S.Ct. 2793, 111 L.Ed.2d 148 (1990).....	8
<i>In re Teddington</i> , 116 Wn.2d 761, 808 P.2d 156 (1991).....	17
<i>State v. Afana</i> , 169 Wn.2d 169, 233 P.3d 879 (2010).....	8
<i>State v. Bradley</i> , 105 Wn.2d 898, 719 P.2d 546 (1986).....	17
<i>State v. Eisfeldt</i> , 163 Wn.2d 628, 185 P.3d 580 (2008).....	8, 11, 18
<i>State v. Gimarelli</i> , 105 Wn. App. 370, 20 P.3d 430 (2001).....	17, 19
<i>State v. Gunwall</i> , 106 Wn.2d 54, 720 P.2d 808 (1986).....	10
<i>State v. Gwinner</i> , 59 Wn. App. 119, 796 P.2d 728 (1990).....	17
<i>State v. Hendrickson</i> , 129 Wn.2d 61, 917 P.2d 563 (1996).....	8, 12
<i>State v. Hinton</i> , 179 Wn.2d 862, 319 P.3d 9 (2014).....	9, 10
<i>State v. Jorden</i> , 160 Wn.2d 121, 156 P.3d 893 (2007).....	9
<i>State v. Martinez</i> , 2 Wn. App. 2d 55, 408 P.3d 721 (2018).....	17

<i>State v. McKinney</i> , 148 Wn.2d 20, 60 P.3d 46 (2002).....	7, 8
<i>State v. Mezquia</i> , 129 Wn. App. 118, 118 P.3d 378 (2005).....	16, 17
<i>State v. Miles</i> , 160 Wn.2d 236, 156 P.3d 864 (2007).....	8
<i>State v. Mollica</i> , 114 N.J. 329, 554 A.2d 1315 (1989).....	17
<i>State v. Myrick</i> , 102 Wn.2d 506, 688 P.2d 151 (1984).....	11
<i>State v. Peppin</i> , 186 Wn. App. 901, 347 P.3d 906 (2015).....	14, 15
<i>State v. Valdez</i> , 167 Wn.2d 761, 224 P.3d 751 (2009).....	8
<i>State v. Winterstein</i> , 167 Wn.2d 620, 220 P.3d 1226 (2009).....	15
<i>State v. Young</i> , 123 Wn.2d 173, 867 P.2d 593 (1994).....	15
<i>United States v. Ackerman</i> , 831 F.3d 1292, 1299 (10th Cir 2016) .....	18
<i>United States v. Cameron</i> , 699 F.3d 621 (1st Cir. 2012).....	18
<i>United States v. Jones</i> , 565 U.S. 400, 415, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012).....	9

**Court Rules and Statutes**

RAP 2.5(a)(3).....	6
--------------------	---

RAP 13.4.....4, 5, 11, 16  
18 U.S.C. § 2258A.....2

**Constitutions**

U.S. Const. amend. IV .....7  
Wash. Const. art. I, § 7.....6, 8

## **I. IDENTITY OF PETITIONER**

Jorden D. Knight, the Appellant, asks this Court to accept review of the Court of Appeals decision terminating review designated in Part II of this motion.

## **II. COURT OF APPEALS DECISION**

Mr. Knight seeks review of the unpublished decision of the Court of Appeals issued on January 19, 2021. A copy of this decision is attached, see App. at 1-12.

## **III. ISSUES PRESENTED FOR REVIEW**

1. Should this Court grant review and reverse when Vancouver Police searched Mr. Knight's Dropbox files without a warrant and with no proof that Mr. Knight shared these files with the public?
2. Does the silver platter doctrine apply when Mr. Knight's files were funneled from a private entity, through a federal nonprofit, to Vancouver Police?

## **IV. STATEMENT OF THE CASE**

Jorden Knight is a Washington resident who resided in the Vancouver area. CP 9. In March 2017, Mr. Knight was charged with five counts of possession of depictions of a minor engaged in sexually explicit conduct. CP 8-11. The charges resulted from an investigation into a cybertip filed by Dropbox, Inc. CP 2.

Dropbox is an internet service provider (ISP) that provides cloud storage services. CP 644. Users can store files with Dropbox and access

these files through the internet from different platforms, such as phones, laptops, or computers. *Id.*

ISPs, including Dropbox, are required by federal law to monitor their users and report certain crimes. 18 U.S.C. § 2258A. ISPs must report suspected sexual exploitation of children to the National Center for Missing and Exploited Children (NCMEC). 18 U.S.C. § 2258A(a)(1)(B). Failure to report can result in hundreds of thousands of dollars in fines. 18 U.S.C. § 2258A(e).

On March 23, 2016, Dropbox contacted NCMEC to report suspected child pornography stored by one of its users. CP 2. Dropbox provided files allegedly containing sexually explicit images of children, as well as data about the account user. *Id.* NCMEC determined that the account originated near Vancouver, Washington, and contacted the Seattle Police, who forwarded the cybertip to the Vancouver Police. *Id.*

Vancouver Police began an investigation of the Dropbox cybertip. CP 2-6. Without a warrant, police opened three of the Dropbox files. CP 2-3. According to police, the files contained sexually explicit images of children. *Id.* Police reviewed the Dropbox account username and email address and focused their investigation on Jordan Knight. CP 3-4. Based on the three files opened without a warrant, police obtained search warrants for information on Mr. Knight from Comcast, Dropbox, and Google. CP 4-

5. Police also obtained a search warrant for Mr. Knight's residence in Camas, Washington. CP 5.

On March 15, 2017, police executed the search warrant of Mr. Knight's residence. RP at 162. Police questioned Mr. Knight and seized his electronics, including a cell phone. RP at 166. On the cell phone, police found numerous files in unallocated space, which meant that the files had been deleted from the cell phone. RP 204-05. These files included five images of children engaged in sexually explicit conduct. RP 211-12, 215-16, 218. The files also included videos, additional images, and messages from an application called Kik. RP 219, 232-35. Kik is a social-media app used to exchange text messages, images, or videos. RP 224. Users can chat one-on-one or can enter a chat group. *Id.* The Kik messages on Mr. Knight's phone appeared to show discussions about sharing sexually explicit images of children. Ex. 16.

In March 2017, Mr. Knight was charged with five counts of possession of depictions of a minor engaged in sexually explicit conduct. CP 8-11. Mr. Knight filed numerous motions to suppress evidence. CP 30-345. He filed an initial motion to suppress all evidence derived from the Dropbox cybertip. CP 30-172. The trial court denied this motion. CP 693. The court determined that Dropbox was a private entity, not a government agent. RP 20; CP 692. The court concluded that NCMEC was a federal



agency, and its warrantless search was consistent with the Fourth Amendment because it did not expand the private search conducted by Dropbox. *Id.* Relying on the “silver platter doctrine,” the court determined that NCMEC properly passed the evidence from Dropbox on to state officials, and state officials did not coordinate with NCMEC prior to obtaining the cybertip. RP 105-06; CP 692-93.

The case proceeded to a bench trial in May 2019. RP 145. The trial court found Mr. Knight guilty of all five counts of first-degree possession of depictions of a minor engaged in sexually explicit conduct. CP 837-51. Mr. Knight appealed. CP 887. The Court of Appeals reversed some of Mr. Knight’s community custody conditions but upheld the search of his Dropbox files as valid. App. at 1. Mr. Knight seeks review.

**V. ARGUMENT WHY REVIEW SHOULD BE ACCEPTED**

Mr. Knight respectfully requests that the Washington Supreme Court grant review and reverse the Court of Appeals. This Court grants review under four circumstances:

- (1) If the decision of the Court of Appeals is in conflict with a decision of the Supreme Court; or
- (2) If the decision of the Court of Appeals is in conflict with a published decision of the Court of Appeals; or
- (3) If a significant question of law under the Constitution of the State of Washington or of the United States is involved; or
- (4) If the petition involves an issue of substantial public interest that should be determined by the Supreme Court.

RAP 13.4(b). Here, review is appropriate under subsections (1), (3) and (4).

This case impacts the electronic privacy concerns of all Washingtonians. Like many people, Mr. Knight stored files with Dropbox, a private entity. Dropbox searched his files and filed a cybertip with NCMEC, a nonprofit receiving federal funding. CP 691. NCMEC forwarded the cybertip and files to Seattle Police, who forwarded them to Vancouver Police. *Id.*

Without a warrant, Vancouver Police searched three of Mr. Knight's Dropbox files and determined that they contained sexually explicit depictions of minors. CP 2-3. Vancouver Police then applied for, and obtained, warrants for Dropbox, Google, Comcast, and Mr. Knight's residence. CP 4-5. The search of Mr. Knight's residence led to the confiscation of his cell phone, which contained the images underlying his convictions. CP 837-41.

This Court should grant review and reverse because the initial warrantless search of Mr. Knight's Dropbox files by Vancouver Police violated article I, section 7 of the Washington Constitution. This issue was preserved from review and involves a significant question of constitutional law. The Court of Appeals erred because its decision dramatically increased the scope of warrantless electronic searches.

**A. Mr. Knight Preserved his Challenge to the Warrantless Search Conducted by Vancouver Police in this Case.**

As an initial matter, Mr. Knight preserved his challenge to the warrantless search of his Dropbox files conducted by Vancouver Police. During the course of these proceedings, Mr. Knight filed numerous motions to suppress evidence, challenging different facets of the searches that led to these charges. RP at 1, 52, 65, 72, 77, 83. He specifically argued that “the silver platter doctrine doesn’t apply” because “the connections between NCMEC and Vancouver Police” prove that these entities are “interrelated police agencies.” RP at 104.

Thus, Mr. Knight did challenge the actions of the Vancouver Police in this case and did preserve this issue for review. Even if he did not, this warrantless search violated Mr. Knight’s right to privacy guaranteed by article I, section 7 of the Washington Constitution, which states, “No person shall be disturbed in his private affairs, or his home invaded, without authority of law.” Wash. Const. art. I, § 7. The issue is appropriate for review because the warrantless search was a manifest error affecting a constitutional right. RAP 2.5(a)(3).

**B. The Warrantless Search by Vancouver Police Violated Mr. Knight’s Constitutional Right to Privacy.**

This Court should grant review and reverse because Vancouver Police conducted a warrantless search of Mr. Knight’s Dropbox files. The

state presented no evidence that Mr. Knight shared these Dropbox files with anyone when Vancouver Police searched them, thus these files were still private and protected. Additionally, no exception to the warrant requirement applies. The “silver platter doctrine” does not apply to private searches of Washington residents that were merely funneled through a nonprofit receiving federal funding. All evidence derived from this illegal search must be suppressed.

**1. The Washington Constitution broadly protects privacy interests.**

Vancouver Police searched Mr. Knight’s Dropbox files without a warrant. This search was presumptively improper under article I, section 7 of the Washington Constitution, which broadly protects privacy.

Although they protect similar interests, “the protections guaranteed by article I, section 7 of the state constitution are qualitatively different from those provided by the Fourth Amendment to the United States Constitution.” *State v. McKinney*, 148 Wn.2d 20, 26, 60 P.3d 46 (2002). The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend. IV. If a government action intrudes on an individual’s “reasonable expectation of privacy,” a search occurs under

the Fourth Amendment. *Illinois v. Rodriguez*, 497 U.S. 177, 187, 110 S.Ct. 2793, 111 L.Ed.2d 148 (1990).

By contrast, the Washington Constitution states, “No person shall be disturbed in his private affairs, or his home invaded, without authority of law.” Wash. Const. art. I, § 7. Unlike the Fourth Amendment, the Washington Constitution is “unconcerned with the reasonableness of the search, but instead requires a warrant before any search, reasonable or not.” *State v. Eisfeldt*, 163 Wn.2d 628, 634, 185 P.3d 580 (2008).

Under article I, section 7, there is an almost absolute bar to warrantless seizures, with only limited, “jealously guarded exceptions.” *State v. Valdez*, 167 Wn.2d 761, 773, 224 P.3d 751 (2009). The burden is always on the state to prove one of these narrow exceptions. *State v. Hendrickson*, 129 Wn.2d 61, 71, 917 P.2d 563 (1996). If the state fails to meet this burden, “violation of [an individual’s] right of privacy under article I, section 7 automatically implies the exclusion of the evidence seized.” *State v. Afana*, 169 Wn.2d 169, 179, 233 P.3d 879 (2010).

To determine whether governmental conduct intrudes on a private affair, Washington courts look at the “nature and extent of the information which may be obtained as a result of the government conduct” and at the historical treatment of the interest asserted. *State v. Miles*, 160 Wn.2d 236, 244, 156 P.3d 864 (2007) (citing *McKinney*, 148 Wn.2d at 29); *see also*,

*e.g.*, *State v. Jordan*, 160 Wn.2d 121, 156 P.3d 893 (2007) (finding random, suspicionless searches of a motel guest registry unconstitutional because those searches may provide “intimate details about a person’s activities and associations”).

Digital documents and communications are protected by article I, section 7. *State v. Hinton*, 179 Wn.2d 862, 319 P.3d 9 (2014). In *Hinton*, this Court held that text messages were private affairs afforded constitutional protection. *Id.* at 869-70. Electronic files, like text messages, expose a “wealth of detail about [a person’s] familial, political, professional, religious, and sexual associations.” *United States v. Jones*, 565 U.S. 400, 415, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (Sotomayor, J., concurring) (discussing GPS (global positioning system) monitoring). These documents “encompass the same intimate subjects as phone calls, sealed letters, and other traditional forms of communication that have historically been strongly protected under Washington law.” *Hinton*, 179 Wn.2d at 869-70. Mr. Knight’s private electronic documents should be afforded similar protections.

The *Hinton* Court also rejected the argument that text messages lost their privacy protections because they were stored by a third party (the recipient). 179 Wn.2d at 873. “Given the realities of modern life, the mere fact that an individual shares information with another party and does not

control the area from which that information is accessed does not place it outside the realm of article I, section 7's protection." *Id.* Washington courts have "consistently declined to require individuals to veil their affairs in secrecy and avoid sharing information in ways that have become an ordinary part of life." *Id.* at 874 (citing *State v. Gunwall*, 106 Wn.2d 54, 67, 720 P.2d 808 (1986) (finding that "[a] telephone is a necessary component of modern life" and "[t]he concomitant disclosure" to the telephone company of the numbers dialed by the telephone subscriber "does not alter the caller's expectation of privacy")). The Court analogized to other instances where private affairs were protected despite third-party access or hosting, including motel registries and banks. *Id.* at 873-74.

Like text messages, hotel registries, and banking records, the fact that Mr. Knight stored his files with a third party—Dropbox—does nothing to lessen their protection as private affairs under article I, section 7. Vancouver Police needed a warrant before searching his files.

**2. Mr. Knight's Dropbox files were protected by article I, section 7 of the Washington Constitution.**

Mr. Knight's also did not waive his privacy rights under article I, section 7. The Court of Appeals determined that Mr. Knight made his Dropbox files "Publicly Available" and thus "did not have a reasonable expectation of privacy in the Dropbox files." App. at 7. The Court

concluded that because he “did not have a reasonable expectation of privacy, Vancouver police did not conduct an unlawful warrantless search when they viewed the three Dropbox files.” *Id.*

At the outset, the Court of Appeals applied the incorrect test under article I, section 7. The Fourth Amendment examines an individual’s reasonable expectation of privacy. *United States v. Jacobsen*, 466 U.S. 109, 119, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984). By contrast, “[u]nlike the Fourth Amendment and its reasonability determination, article I, section 7 protections are not ‘confined to the subjective privacy expectations of modern citizens.’” *Eisfeld*, 163 Wn.2d at 637 (quoting *State v. Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151 (1984)). Instead, article I, section 7 protects “those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass absent a warrant.” *Id.* (quoting *Myrick*, 102 Wn.2d at 511). Washington Courts “have repeatedly held the privacy protected by article I, section 7 survived where the reasonable expectation of privacy under the Fourth Amendment was destroyed.” *Id.* This Court should grant review to correct the Court of Appeals’ error. *See* RAP 13.4(b) (1), (3) and (4).

The Court of Appeals also erred in its factual inferences. The Court determined that Mr. Knight must have shared his Dropbox files because he made them “Publicly Available”:



Here, Dropbox’s CyberTipline Report informed NCMEC that Knight made most of the files in the report “Publicly Available.” In other words, Knight created shareable links to his Dropbox files. ***We infer Knight created the shareable links for distribution and he distributed those links.*** So, he did not have a reasonable expectation of privacy in the Dropbox files.

App. at 7 (emphasis added). The Court concluded that Mr. Knight had no expectation of privacy to these files with shareable links. *Id.*

The Court of Appeals erred because creating “shareable links” in Dropbox does not mean that the files were actually shared with anyone. Dropbox allows users to choose how to designate their files. CP 479. A user can create a “shared link,” which creates a Uniform Resource Locator (“URL”) link to a file. *Id.* The user can then share that URL with other people. *Id.* Shared links are not accessible through search engines<sup>1</sup>—people can only access these files if the user sends them the URL. *Id.*

Here, the state presented no evidence that Mr. Knight shared his Dropbox files with anyone in March 2016, when Vancouver Police conducted its warrantless search. The state bears the burden of proving that this warrantless search was justified. *See Hendrickson*, 129 Wn.2d at 71. The state failed to meet that burden. The only evidence at trial showed that Mr. Knight shared some of his Dropbox files nearly a year later, in February

---

<sup>1</sup> Unless the user posts the URL for the shared file onto another webpage. There is no evidence to suggest that this happened in this case.

and March 2017, though the Kik application. *See* Ex. 16. The state presented no evidence about sharing any files in March 2016.

At trial, there was no testimony about shareable Dropbox links at all. It is unclear how these links are created, what Dropbox sets as the default designation for stored files, or when Mr. Knight designated these files as shareable. Maybe he created shareable links to share these files between his own electronic devices. Maybe he created shareable links in anticipation of sharing these files in the future. Maybe this is just the default designation for Dropbox files. Without more information, the Court of Appeals could not infer that Mr. Knight intended to share his files with other people, let alone that he actually did so.

Even if Mr. Knight intended to share his Dropbox files with other people, the state presented no evidence that this actually happened on or before March 2016. Intending to share a file is not the same as actually sharing it. Suppose Mr. Knight wrote a letter, addressed it, stamped it, and put it in his desk drawer. Under the Court of Appeals' reasoning, Mr. Knight intended to share this letter, so he had no expectation of privacy in its contents, and police could search the letter without a warrant. This Court should reject this inference because it does not protect the privacy interests of Washingtonians consistent with article I, section 7.

The Court of Appeals also erred by relying on *State v. Peppin*, 186 Wn. App. 901, 347 P.3d 906 (2015), a legally and factually distinguishable case. App. at 7. In *Peppin*, police used a peer-to-peer file sharing application to access files on the defendant's computer. 186 Wn. App. at 903-04. The defendant had downloaded this application to his computer and was using it to share sexually explicit files of children over the internet. *Id.* at 906. Police used the application to download files from Mr. Peppin, including videos of children engaged in sexually explicit conduct. *Id.* at 905-06. This Court upheld the search as constitutional. *Id.* at 911. The *Peppin* Court noted that "law enforcement did not gain more information than was available to the public" and did not "intrude into a computer file that Mr. Peppin intended to keep private." *Id.*

*Peppin* is distinguishable for two reasons. First, in this case police did not use a peer-to-peer file sharing application to access Mr. Knight's digital files. CP 2-6. Vancouver Police received the Dropbox cyber tip, viewed three of Mr. Knight's files without a warrant, and then obtained a search warrant for Mr. Knight's electronic devices. CP 2. Police searched Mr. Knight's phone pursuant to this warrant. *Id.* On his phone, police found the Kik messages from February and March 2017 where Mr. Knight shared his Dropbox files with other people. RP 219, 232-35. The fact that an officer could have used the Kik application to chat with Mr. Knight and get

Mr. Knight to share the files directly with that officer is irrelevant. This Court has soundly rejected the inevitable discovery doctrine. *State v. Winterstein*, 167 Wn.2d 620, 220 P.3d 1226 (2009).

Second, *Peppin* is factually distinguishable because in that case, the defendant actually shared the files in question when police accessed them. The *Peppin* Court recognized that article I, section 7 does not protect “information voluntarily held out to the public” because this information is “not considered part of a person’s private affairs.” 186 Wn. App. at 910 (quoting *State v. Young*, 123 Wn.2d 173, 182, 867 P.2d 593 (1994)). In that case, “Mr. Peppin voluntarily offered public access to the computer files obtained by Detective Cestnik,” thus “[l]aw enforcement’s access of these files was not an intrusion into Mr. Peppin’s private affairs.” *Id.*

Here, unlike in *Peppin*, the state presented no evidence that Mr. Knight actually shared his Dropbox files when Vancouver Police conducted its warrantless search in March 2016. A file designation—absent any evidence that the file was actually shared—cannot be enough to remove a file from a person’s private affairs. This is because the file designation alone does not show that this file was “voluntarily held out to the public.” *Peppin*, 186 Wn. App. at 910.

The warrantless search in this case happened months before Mr. Knight shared his Dropbox files via Kik. The state presented no evidence

that Mr. Knight shared any of his Dropbox files in March 2016, when Vancouver Police conducted this warrantless search. These files were thus part of Mr. Knight's private affairs and protected by article I, section 7. Vancouver Police conducted an illegal search by viewing these files without a warrant. This Court should grant review and reverse in order to safeguard the privacy interests of Washingtonians. *See* RAP 13.4(b) (3), (4).

**3. The “silver platter doctrine” does not apply in this case.**

The Court of Appeals also upheld this warrantless search by applying the “silver platter doctrine.” App. at 7-8. The Court erred because the silver platter doctrine does not apply to the private search in this case. This Court should grant review and reverse because Washington does not recognize the private search doctrine. *See* RAP 13.4(b)(1). This Court should also establish that funneling information from a private search through a federal entity cannot evade article I, section 7 protections. *See* RAP 13.4(b) (3), (4).

Under the silver platter doctrine, evidence lawfully obtained under the laws of another jurisdiction is admissible in Washington courts even if the manner the evidence was obtained would violate Washington law. *State v. Mezquia*, 129 Wn. App. 118, 132, 118 P.3d 378 (2005). Courts apply a two-step test. “Evidence is admissible under this doctrine when (1) the foreign jurisdiction lawfully obtained evidence and (2) the forum state’s

officers did not act as agents or cooperate or assist the foreign jurisdiction.”  
*Id.* at 132.

The roots of the silver platter doctrine lie in federalism. The silver platter doctrine developed in federal courts when federal standards for lawful searches and seizures were usually more protective than state standards. *State v. Gwinner*, 59 Wn. App. 119, 124-25, 796 P.2d 728 (1990) (citing *State v. Mollica*, 114 N.J. 329, 346-47, 554 A.2d 1315 (1989)). Consistent with federalist principles, courts concluded that state constitutions do not control the actions of federal officials. *Mollica*, 554 114 N.J. at 350 (citing *State v. Bradley*, 105 Wn.2d 898, 902-03, 719 P.2d 546 (1986)).

In other words, the silver platter doctrine “is based upon the idea that because state constitutions have inherent jurisdictional limits, it would disserve the principles of federalism and comity to subject foreign law enforcement officers to state constitutions.” *State v. Gimarelli*, 105 Wn. App. 370, 380, 20 P.3d 430 (2001) (citing *In re Teddington*, 116 Wn.2d 761, 774, 808 P.2d 156 (1991)). This doctrine has also been applied to evidence seized in other states by state officials. *See State v. Martinez*, 2 Wn. App. 2d 55, 64-65, 408 P.3d 721 (2018) (video seized in Texas by Texas law enforcement and sent to Washington); *Mezquia*, 129 Wn. App.

at 132-33 (DNA sample obtained in Florida by Florida law enforcement and sent to Washington).

The silver platter doctrine should not apply in this case. The trial court found that Dropbox acted as a private entity, not an agent of federal law enforcement. CP 692. Principles of federalism and comity have no bearing on evidence seized by a private entity in Washington, from a Washington resident. This Court has “adopted a bright line rule” holding the private search doctrine “inapplicable under article I, section 7 of the Washington Constitution.” *Eisfeldt*, 163 Wn.2d at 638.

Filtering Dropbox’s private search through NCMEC also did not trigger the silver platter doctrine. NCMEC is a nonprofit organization. *United States v. Cameron*, 699 F.3d 621, 628 (1st Cir. 2012). It receives the bulk of its funding from the federal government and is required by federal law to “operate the official national clearinghouse for information about missing and exploited children.” *United States v. Ackerman*, 831 F.3d 1292, 1296, 1299 (10th Cir 2016). Courts have held that NCMEC is a government entity for the purposes of the Fourth Amendment. *See Id.*, 831 F.3d at 1297; *Cameron*, 699 F.3d at 645.

The Court of Appeals found that NCMEC is an “an arm of federal law enforcement,” and thus the silver platter doctrine applies. App. at 9. The Court erred because NCMEC did not conduct a federal investigation in

this case. NCMEC received the cybertip and files from Dropbox. CP 2. It viewed only two files before forwarding all 322 to Washington law enforcement. *Id.* NCMEC “does not investigate” crimes, and “cannot verify the accuracy of the information submitted by reporting parties,” nor did it attempt to do so in this case. CP 357. This case does not raise the danger of “subject[ing] foreign law enforcement officers to state constitutions.” *Gimarelli*, 105 Wn. App. at 380.

Article I, section 7 is not so easily evaded. Washington residents should not be stripped of their constitutional protections by merely funneling evidence through a federal entity that conducted no law enforcement functions. This Court should grant review, reverse, and hold that the silver platter doctrine does not apply to private searches of Washington residents just because the evidence passed through a clearinghouse created by federal law.

## VI. CONCLUSION

Mr. Knight respectfully requests that the Washington Supreme Court grant review and reverse the Court of Appeals.

RESPECTFULLY SUBMITTED this 18th day of February, 2021.



---

STEPHANIE TAPLIN

WSBA No. 47850

Attorney for Appellant, Jorden Knight



**VII. APPENDIX**

Court of Appeals, Division One, Unpublished Opinion  
January 19, 2021 .....1-12

IN THE COURT OF APPEALS FOR THE STATE OF WASHINGTON

STATE OF WASHINGTON,  
  
Respondent,  
  
v.  
  
JORDEN D. KNIGHT,  
  
Appellant.

No. 81837-6-I  
  
DIVISION ONE  
  
UNPUBLISHED OPINION

LEACH, J. — Jordan David Knight appeals his convictions for five counts of first degree possession of depictions of a minor engaged in sexually explicit conduct. Knight argues Vancouver police conducted an unlawful warrantless search of the Dropbox files it received from the National Center for Missing and Exploited Children. We disagree and affirm. Knight also argues, and the State concedes, the trial court should not have imposed conditions of community custody prohibiting him from entering into certain romantic relationships and requiring him to submit to urine and breath testing for alcohol. We agree and remand to strike those conditions from the judgment and sentence.

BACKGROUND

On March 23, 2016, Dropbox, Inc. informed the National Center for Missing and Exploited Children (NCMEC) that Jordan Knight was using its digital storage

service to “posses[], manufacture, and distribut[e]” files depicting minors engaged in sexually explicit activity by filing CyberTipline Report 9052622.

Dropbox is a digital cloud storage and file sharing company. Its users upload and store files in their Dropbox accounts. “A Dropbox user who creates a shared link for a file can then share that file with others by distributing the URL for the shared link. Any member of the public who clicks on that link or who otherwise accesses the shared link’s URL can view the associated file without logging into a Dropbox account.” “Shared links for files uploaded to Dropbox are not accessible through search engines unless the user posts the link on a page that is otherwise accessible through search engines.” “When Dropbox indicates in a CyberTipline report that a file was ‘Publicly Available,’ Dropbox is referring to the fact that a shared link was created for that file.”

The CyberTipline report included 322 files from Knight’s Dropbox account. Dropbox indicated that most of the files were “Publicly Available.”

When Dropbox discovers files depicting minors engaged in sexually explicit activity, its content safety team reviews the files to determine whether they violate their Terms of Service and Acceptable Use Policy<sup>1</sup> and meets the definition of child pornography under 18 U.S.C. § 2256. If Dropbox determines the files qualify as

---

<sup>1</sup> Dropbox’s privacy policy states, we may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request; (b) protect the safety of any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or its users; or (d) to protect Dropbox’s property rights.

apparent child pornography, it creates a "CyberTipline" report and sends it to NCMEC.

NCMEC determined Knight lived in Vancouver, Washington. It sent a "cybertip," including files and data, to the Internet Crimes Against Children (ICAC) task force in Seattle. ICAC assigned the tip to the Vancouver Police Digital Evidence Cybercrime Unit (DECU). Without a warrant, DECU Detective Robert Givens accessed the 322 files and reviewed three of them in detail. The files contained child pornography. Based on these files, Vancouver police obtained warrants to search Knight's Comcast, Dropbox, and Google accounts. Police obtained a warrant to place a GPS tracking device on Knight's teal 1995 Ford Escort. Police also obtained a warrant to search Knight's home, car, and any devices and data found for evidence of the crime.

On March 15, 2017, while Knight was home police executed the search warrant for Knight's home and car. Police knocked on Knight's door and announced they were the police and had a search warrant. Five minutes after police entered Knight's home, he walked upstairs from the basement and met the police. Police seized Knight's cell phone, two laptop computers, and two thumb drives. Police arrested Knight.

DECU Investigator Christopher Prothero conducted a forensic analysis of Knight's cell phone. Knight's name, email addresses, and Dropbox account were associated with the phone. Investigator Prothero recovered pornographic images and videos of minors that had been deleted from the phone. He also recovered

numerous conversations in a social media application called Kik. Investigator Prothero discovered Kik was downloaded to the phone using Knight's email address. He recovered deleted Kik conversations where Knight exchanged child pornography files and Dropbox links to files with pornographic names with other Kik users. One message Knight sent stated, "I told you LOL I have three hundred plus Dropbox vids of boys and girls and can even take lives of me but you have to offer something good to get." In another message he stated, "Have tons of Dropbox links and vids like this, just making sure you have them too. Boys, girls, mi." Investigator Prothero compared the files on the phone to the Dropbox files provided by NCMEC and found that none of the files were the same.

The State charged Knight with five counts of possession of depictions of a minor engaged in sexually explicit activity in the first degree under RCW 9.68A.070(1).

Knight asked the trial court to suppress evidence obtained from Comcast, Dropbox, Google, GPS, and his home, car, and cell phone. Knight also requested the court exclude the Kik messages. The court granted his GPS request, denied his other requests, and admitted the evidence seized at Knight's home. Knight also asked the court to dismiss the case. The court denied the request.

On May 15, 2019, the trial court convicted Knight on all five counts of possession of depictions of a minor engaged in sexually explicit conduct in the first degree. The standard sentencing range was between 77 and 102 months. The court imposed a sentence of 77 months. The court also imposed a number of

community custody conditions. These included conditions prohibiting Knight from possessing or consuming alcohol and entering into “a romantic relationship with another person who has minor children in their care or custody.”

Knight appeals.

## ANALYSIS

### File Search

Knight asserts Vancouver police conducted an illegal warrantless search when it reviewed three of the Dropbox files it obtained from NCMEC. The State argues Knight waived this claim by not raising it at trial.

Generally, an appellate court will not review issues raised for the first time on appeal.<sup>2</sup> A recognized exception to this rule allows review if the appellant shows a “manifest error affecting a constitutional right.”<sup>3</sup>

To establish a manifest constitutional error, the appellant must identify a constitutional error and make a showing the error likely prejudiced their rights at trial.<sup>4</sup> “It is this showing of actual prejudice that makes the error ‘manifest,’ allowing appellate review.”<sup>5</sup> “Thus, a court previews the merits of the constitutional argument first raised on appeal to determine if it is likely to succeed.”<sup>6</sup>

Knight argues Vancouver police violated article I, section 7 of the Washington State Constitution by searching three Dropbox files without a warrant

---

<sup>2</sup> RAP 2.5(a).

<sup>3</sup> RAP 2.5(a)(3).

<sup>4</sup> State v. Kirkman, 159 Wn.2d 918, 926-27, 155 P.3d 125 (2007).

<sup>5</sup> Kirkman, 159 Wn.2d at 927 (citing State v. McFarland, 127 Wn.2d 322, 333, 899 P.2d 1251 (1995)).

<sup>6</sup> State v. Reeder, 181 Wn. App. 897, 912, 330 P.3d 786 (2014).

and that no exception to the warrant requirement applies. Article I, section 7 provides, “No person shall be disturbed in his private affairs, or his home invaded, without authority of law.” “This provision prohibits the State from unreasonably intruding on a person’s private affairs and places a greater emphasis on the right to privacy than the Fourth Amendment to the United States Constitution does.”<sup>7</sup> “Generally, officers of the State must obtain a warrant before intruding into the private affairs of others, and we presume that warrantless searches violate both [Washington State and United States] constitutions.”<sup>8</sup> The State bears the burden of overcoming this presumption and demonstrating the warrantless search fell under a narrow exception to the warrant requirement.<sup>9</sup>

The State argues Vancouver police did not need a warrant to review the three Dropbox files it received because Knight did not have a reasonable expectation to privacy when he previously created sharable Dropbox links. Washington courts do not extend article I, section 7 protections to information voluntarily held out to the public.<sup>10</sup> “[W]hat is voluntarily exposed to the general public and observable without the use of enhancement devices from an unprotected area is not considered part of a person's private affairs.”<sup>11</sup>

---

<sup>7</sup> Reeder, 181 Wn.2d at 912 (citing State v. Young, 123 Wn.2d 173, 179, 867 P.2d 593 (1994) (citing State v. Stroud, 106 Wn.2d 144, 148, 720 P.2d 436 (1986); State v. Simpson, 95 Wn.2d 170, 178, 622 P.2d 1199 (1980); State v. Chacon Arreola, 176 Wn.2d 284, 291, 290 P.3d 983 (2012)).

<sup>8</sup> State v. Villela, 194 Wn.2d 451, 456, 450 P.3d 170 (2019) (quoting State v. Day, 161 Wn.2d 889, 893, 168 P.3d 1265 (2007)).

<sup>9</sup> Villela, 194 Wn.2d at 458.

<sup>10</sup> State v. Peppin, 186 Wn. App. 901, 910, 347 P.3d 906 (2015).

<sup>11</sup> Peppin, 186 Wn. App. at 910 (quoting State v. Young, 123 Wn.2d 173, 182, 867 P.2d 593 (1994)).

In State v. Peppin,<sup>12</sup> police used file sharing software to access three digital files depicting child pornography that Peppin shared.<sup>13</sup> Peppin was convicted of first degree possession of depictions of a minor engaged in sexually explicit conduct.<sup>14</sup> On appeal, Peppin argued he had a reasonable expectation to privacy in his computer files and police violated his Washington State Constitution article I, section 7 and Fourth Amendment rights.<sup>15</sup> We determined Peppin did not have a constitutionally protected right to privacy in the files because he shared them with the public.<sup>16</sup>

Here, Dropbox's CyberTipline Report informed NCMEC that Knight made most of the files in the report "Publicly Available." In other words, Knight created sharable links to his Dropbox files. We infer Knight created the shareable links for distribution and he distributed those links. So, he did not have a reasonable expectation of privacy in the Dropbox files. And, because Knight did not have a reasonable expectation of privacy, Vancouver police did not conduct an unlawful warrantless search when they viewed the three Dropbox files. The State has met its burden of demonstrating the warrantless search fell under a narrow exception to the warrant requirement.

The State also argues that even if the exception to the warrant requirement does not apply, the private search doctrine applies to NCME and the silver platter

---

<sup>12</sup> 186 Wn. App. 901, 347 P.3d 906 (2015).

<sup>13</sup> Peppin, 186 Wn. App. at 903-06.

<sup>14</sup> Peppin, 186 Wn. App. at 903.

<sup>15</sup> Peppin, 186 Wn. App. at 903.

<sup>16</sup> Peppin, 186 Wn. App. at 910.



doctrine applies to police, so police legally viewed the files and the files were properly admitted at trial. We agree.

“Under the private search doctrine a warrantless search by a state actor does not offend the Fourth Amendment if the search does not expand the scope of the private search.”<sup>17</sup> “Underlying this doctrine is the rationale that an individual’s reasonable expectation of privacy is destroyed when the private actor conducts his search.”<sup>18</sup> The private search doctrine does not apply in Washington.<sup>19</sup> But, the silver platter doctrine provides that “evidence lawfully obtained under the laws of another jurisdiction is admissible in Washington courts even if the evidence was obtained in a manner that would violate Washington law.”<sup>20</sup>

Here, Dropbox, a private entity, conducted a search of Knight’s Dropbox files. Dropbox’s privacy policy permits it to conduct searches of its users’ files. Under the private search doctrine, Dropbox’s search destroyed Knight’s reasonable expectation of privacy. NCMEC, a federal government agency not governed by article I, section 7 received and reviewed the files Dropbox sent. NCMEC’s review did not expand the scope of the Dropbox’s search. So, under the private search doctrine, NCMEC’s review of the three files was lawful.

---

<sup>17</sup> State v. Eisefeldt, 163 Wn.2d 628, 636, 185 P.3d 580 (2008).

<sup>18</sup> Eisefeldt, 163 Wn.2d at 636 (citing United States v. Jacobsen, 466 U.S. 109, 119, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984)).

<sup>19</sup> Eisefeldt, 163 Wn.2d at 636.

<sup>20</sup> State v. Martinez, 2 Wn. App. 2d 55, 64, 408 P.3d 721 (2018).

Because NCMEC sent the files to Vancouver police for review, the silver platter doctrine applies. “Evidence is admissible under this doctrine when (1) the foreign jurisdiction lawfully obtained evidence and (2) the forum state’s officers did not act as agents or cooperate or assist the foreign jurisdiction.”<sup>21</sup> The trial court found NCMEC lawfully obtained the Dropbox files from Dropbox and that the Vancouver police did not act as NCMEC’s agent or cooperate or assist in obtaining the Dropbox files. Knight does not contend the contrary on appeal. Instead, he contends NCMEC is not a law enforcement agency of a foreign jurisdiction covered by the silver platter doctrine. We disagree. NCMEC has broad federal law enforcement powers under two primary statutes 18 U.S.C. § 2258 and 34 U.S.C. § 11293. NCMEC is statutorily obligated to operate the official national clearinghouse for information about missing and exploited children to help law enforcement locate and recover those children, to track and identify patterns of attempted child abductions, and to operate the CyberTipline as a means of combating Internet child sexual exploitation.<sup>22</sup> It must maintain the electronic tip line for Internet Service Providers (ISPs) to use to report possible Internet child sexual exploitations to the government and must forward every single report it receives to federal law enforcement agencies.<sup>23</sup> The argument that NCMEC is not an arm of federal law enforcement is without merit.

---

<sup>21</sup> Martinez, 2 Wn. App. 2d at 64.

<sup>22</sup> 34 U.S.C. § 11293.

<sup>23</sup> 18 U.S.C. § 2258.

So, Vancouver police lawfully reviewed the three files and obtained warrants before conducting additional searches. Because Vancouver police did not conduct an unconstitutional warrantless search of the Dropbox files, the trial court properly admitted those files and derivative evidence.

After previewing the merits of Knight's constitutional argument and the State's response, we determine Knight cannot demonstrate a manifest error affecting a constitutional right. We affirm.

Because Knight cannot show any unlawful search, we need not reach the State's contraband, term of use, and independent source arguments supporting its position.

#### Community Custody Conditions

Knight appeals the following community custody conditions.

4. You shall refrain from possessing or consuming alcohol without prior approval from DOC and all treatment providers. RCW 9.94A.703(3)(e).

5. You shall submit to urine, breath, PBT/BAC, or other monitoring whenever requested to do so by your community corrections officer to monitor compliance with abstention from alcohol and non-prescribed controlled substances.

[ . . . ]

11. You shall not enter into a romantic relationship with another person who has minor children in their care or custody without prior approval of DOC and your sexual deviancy treatment provider.

The State concedes the trial court's imposition of community custody conditions prohibiting Knight from entering into certain romantic relationships and

requiring Knight submit to urine and breath testing for alcohol were in error. We accept the concessions and remand to strike those conditions.

Statement of Additional Grounds

Knight claims two errors in his pro se statement of additional grounds. A defendant may file a pro se statement of additional grounds for review to identify and discuss those matters the defendant believes have not been adequately addressed by counsel.<sup>24</sup> “Reference to the record and citation to authorities are not necessary or required, but the appellate court will not consider a defendant’s statement of additional grounds for review if it does not inform the court of the nature and occurrence of alleged errors.”<sup>25</sup> And, we are not obligated to search the record for support of claims made in a defendant’s statement of additional grounds for review.<sup>26</sup>

First, Knight argues the trial court unfairly imposed an excessive sentence. RCW 9.94A.585 allows a defendant sentenced to an exceptional sentence to challenge it as excessive but prohibits a defendant from appealing a sentence within the standard range. The standard sentence range here was 77 to 102 months. And, the trial court imposed the low end of the range at 77 months. So, Knight cannot appeal this sentence.

Second, Knight challenges RCW 9.68A.070 claiming it authorizes courts to impose excessive and unlawful punishment. We presume the statute


---

<sup>24</sup> RAP 10.10(a).  
<sup>25</sup> RAP 10.10(c).  
<sup>26</sup> RAP 10.10(c).

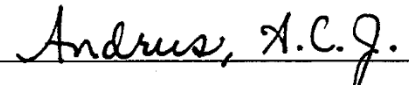
constitutional, and the burden is on Knight to prove otherwise.<sup>27</sup> Knight has presented no persuasive argument that the statute is unconstitutional, so this claim fails.

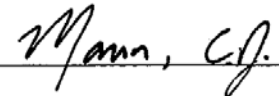
CONCLUSION

Because the police lawfully reviewed the Dropbox files before obtaining search warrants, we affirm Knight's convictions for possession of depictions of a minor engaged in sexually explicit conduct in the first degree. We remand to the trial court to strike the conditions of community custody prohibiting Knight from entering into certain "romantic relationships" and requiring Knight to submit to urine and breath testing for alcohol.

  
\_\_\_\_\_  
Judge Pro Tempore

WE CONCUR:

  
\_\_\_\_\_

  
\_\_\_\_\_

---

<sup>27</sup> State v. McCuiston, 174 Wn.2d 369, 387, 275 P.3d 1092 (2012).

Supreme Court No. (to be set)  
Court of Appeals No. 81837-6-I

CERTIFICATE OF SERVICE

I, Stephanie Taplin, declare under penalty of perjury under the laws of the State of Washington that the following is true and correct to the best of my knowledge:

On February 18, 2021, I electronically filed a true and correct copy of the **Petition for Review by the Appellant, Jordan D. Knight**, via the Washington State Appellate Courts' Secure Portal to the Washington Court of Appeals, Division I. I also served said document as indicated below:


Aaron Bartlett,  
Clark County Prosecuting  
Attorney's Office

( X ) via email to:  
aaron.bartlett@clark.wa.gov;  
CntyPA.GeneralDelivery@clark.wa.gov

Jorden D. Knight  
DOC # 415305  
Monroe Correctional  
Complex  
PO Box 7001  
Monroe, WA 98272

( X ) via U.S. mail

SIGNED in Park City, Utah, this 18th day of February, 2021.

  
\_\_\_\_\_  
STEPHANIE TAPLIN  
WSBA No. 47850  
Attorney for Appellant, Jorden D.  
Knight

**NEWBRY LAW OFFICE**

**February 18, 2021 - 2:52 PM**

**Transmittal Information**

**Filed with Court:** Court of Appeals Division I  
**Appellate Court Case Number:** 81837-6  
**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:**

- 818376\_Petition\_for\_Review\_20210218144701D1632696\_9615.pdf  
This File Contains:  
Petition for Review  
*The Original File Name was Knight PFR SCt.pdf*

**A copy of the uploaded files will be sent to:**

- CntyPA.GeneralDelivery@clark.wa.gov
- aaron.bartlett@clark.wa.gov

**Comments:**

---

Sender Name: Stephaie Taplin - Email: stephanie@newbrylaw.com

Address:

623 DWIGHT ST

PORT ORCHARD, WA, 98366-4619

Phone: 360-876-5477

**Note: The Filing Id is 20210218144701D1632696**