STATE OF WISCONSIN
COURT OF APPEALS
DISTRICT IV

Appeal No. 2022 AP 002051 CR

**STATE OF WISCONSIN,**

Plaintiff-Respondent,

vs.

**JACOB R. BEYER,**

Defendant-Appellant.

# BRIEF AND APPENDIX OF DEFENDANT-APPELLANT

On Appeal from Orders of the Court Denying Defendant's Pretrial Motions and from the Judgment of Conviction and Sentence dated July 23, 2019, in the Circuit Court for Dane County, the Honorable William E. Hanrahan Presiding, Trial Court Case No 17-CF-2831, and from the Judgment of Conviction entered after a trial to the Court on August 30, 2022, in the Circuit Court for Dane County, the Honorable Mario D. White Presiding, Case No. 17-CF-2831

Mark A. Eisenberg
State Bar Number: 01013078
EISENBERG LAW OFFICES, S.C.
308 E. Washington Avenue
P. O. Box 1069
Madison, WI 53701-1069
(608) 256-8356
Attorneys for Defendant-Appellant
Jacob R. Beyer

TABLE OF CONTENTS

**Page**

UNPUBLISHED AUTHORITIES:

## TABLE OF AUTHORITIES

**Cases** **Page**

**Statutes**

**Other Materials**

## ISSUES PRESENTED FOR REVIEW

(1) Did the trial court err in denying Beyer's request for an order permitting forensic analysis of the investigative computer that allegedly detected a file containing child pornography which served as the chief premise for law enforcement's application for warrant to search Beyer's home and electronic devices?

The search warrant alleged that the State's undercover investigative computer software("UIS") established a peer-to-peer ("P2P") connection with a device at Beyer's registered internet protocol ("IP") address and subsequently executed a single-source download of a single file containing child pornography from the publicly accessible "shared" contents of that device. Though that allegedly illicit file could not be recovered after the execution of a search warrant at Beyer's residence, and despite the parties' apparent agreement that its existence at the relevant place and time could likely be ascertained via forensic analysis of the investigative computer, the trial court denied Beyer's discovery motion on the grounds that Wis. Stat. § 971.23 did not entitle Beyer to discovery of this evidence as the State did not intend to use it at trial in spite of Beyer's invocation of his constitutional right to the discovery pursuant to the guarantees of due process.

(2) Did the affidavit in support of the application for the search warrant of Beyer's home and electronic devices fail to establish probable cause by virtue of its deliberately misleading information about offenders' propensity for collecting child pornography; its failure to provide any specific corroborative information about Beyer linking him to any such category of offenders; and its failure to provide relevant information regarding the reliability of the undercover investigative software ("UIS") at issue?

The application for the search warrant in this case explicitly averred that the recovery of illicit files from Beyer's electronic devices by law enforcement could "reasonably be expected" due to the tendency of offenders to collect or retain child pornography that they have procured. However, during a motion hearing, the applicant provided testimony that indicated that this representation was inaccurate and overbroad. He suggested that the passage of time, as opposed to any widespread behavioral trend, is the crucial consideration in predicting whether a given file detected by UIS will be recovered. Furthermore, he acknowledged that, at the time of the application, he did not possess any information suggesting that Beyer was a likely "collector" other than the single file of child pornography detected by the UIS. Despite expressing some reservations in light of the applicant's testimony, the trial court found the search warrant was supported by probable cause and that suppression under the Fourth Amendment was unwarranted due to a lack of foreseeable prophylactic value with respect to future law enforcement conduct.

(3) Was there sufficient evidence presented at the court trial to enable the trial court to make a finding beyond a reasonable doubt that Beyer knowingly possessed child pornography as alleged in Count 1 of the Information?

Despite a dearth of testimony indicating that Beyer ever accessed or viewed the relevant image and his corresponding contention that there was insufficient evidence from which the court could conclude beyond a reasonable doubt that he was guilty of knowingly possessing child pornography as delineated in count 1 of the information, the court indicated that there was circumstantial evidence which allowed it to find Beyer guilty.

## POSITION ON ORAL ARGUMENT AND PUBLICATION

Beyer requests the opportunity to present oral argument if the Court finds that the parties' positions require further elucidation or supplementation to clear up any specific questions from the Court which may have been unanticipated or unaddressed by the parties in their briefs. Beyer also believes that publication is necessary in order to provide clarity at the intersection of technological advancements in the use of investigation software and constitutionally enshrined rights of individual persons.

## STATEMENT OF THE CASE

On October 28, 2017, between 9:53 a.m. and 9:55 a.m., Special Agent Lenzner of the Wisconsin Department of Justice Criminal Division, through the utilization of undercover investigative software ("UIS") on a peer-to-peer ("P2P") BitTorrent network, allegedly downloaded a single video file which he subsequently identified as child pornography from a "Suspect Device" connected to the network with IP Address 71.90.79.138. (R.55:15-25). On October 30, 2017, Agent Lenzner submitted an administrative subpoena to Charter Communications for subscriber information for the IP address associated with the downloaded file. (R.55:15). On November 21, 2017, Charter Communications responded to the subpoena and indicated that the subscriber for that particular address was Jacob Beyer, who lived in a multi-unit apartment building located at 7237 Tempe Drive in Madison, Wisconsin. (R.55:15).

On December 4, 2017, the State conducted surveillance and confirmed that Beyer was living at that residence. (R.55:16). On December 6, 2017, the State applied for a search warrant, chiefly premising the application upon the alleged acquisition of the single file of child pornography through the State's UIS (Roundup Torrential Downpour Receptor) and a description of the video content. The application also included a summary explanation of how child pornography may be tracked and/or disseminated through P2P networks, as well as a general representation that the investigatory ambit of the UIS is limited to the "shared" folders of other peers on the network which are otherwise publicly accessible for all network users. (R.55). Finally, the application averred that there was a "fair

probability" of recovering the contraband digital data even after "the passage of long periods of time" because

> individuals who have an interest in child pornography or child sexual exploitation tend to retain any images or videos they obtain that depict such activity or maintain their interest in such depiction so it can be reasonably expected that similar evidence of that sexual interest in children or interest in child sexual exploitation will be found in their computer(s) or other digital devices or storage media, or found in other forms in their private places. (R.55:17).

Beyond the representation that a single file of child pornography was obtained from a device traced to Beyer's IP address, the warrant application did not offer any further information to qualify Beyer as a "collector." Moreover, the application did not specify whether there was any indication that Beyer ever opened, viewed, or modified the illicit file in question, nor did it indicate that any other known files of child pornography could be traced to the relevant IP address.[1]

The search warrant was ultimately granted by the Honorable John Hyland, and law enforcement executed a search

---

[1] At the trial on August 30, 2022 the State's forensic expert testified that she could not determine whether Beyer ever knew the illicit file in question was on his device (R.175:46; A:110). At the suppression hearing, the case agent stated he could not tell if Beyer ever looked at the image or knew it was on his computer. (R66:27-28). Knowledge is a necessary element to convict someone of possession of child pornography.

of Beyer's premises on December 7, 2017. (R. 55:19). Based on the contents recovered from Beyer's electronic devices, he was subsequently charged with ten counts of Possession of Child Pornography pursuant to Wis. Stat. 948.12(1m) in a Criminal Complaint filed on December 8, 2017. (R.1).

Beyer filed a "Demand for Additional Discovery and Inspection" on February 26, 2018, which included a request to view the State's computer and UIS that was utilized in the investigation precipitating the Complaint. (R.18). The State refused to accede to this request, and so on December 18, 2018, Beyer formally filed a "Motion to View the State's Computer and Its Undercover Software." (R.50). In his motion, Beyer indicated that his forensic computer expert, Juanluis Villegas, had been permitted to make a copy of Beyer's hard drive at the offices of the Department of Criminal Investigation on October 5, 2018. (R.50:2-3). However, in his subsequent analysis of that hard drive, Villegas had been unable to locate any file with the SHA-1 hash value corresponding with the file allegedly detected by Agent Lenzner on October 28, 2017. (R.50:2-3). Villegas also conducted a search utilizing the State's UIS infohash, as well as a search by file name, both of which also proved fruitless. (R.50:2-3). Accordingly, Beyer asked the trial court for an Order permitting his forensic expert "to look at the State's computer with the hardware and software configuration and settings it had on the dates and times the agent claims he detected the evidence of child pornography" to confirm that the file that Agent Lenzner purportedly viewed did actually exist at the relevant time and location. (R.50:3).

The State subsequently filed a "Motion to Deny the Defense Motion to Inspect," arguing that Beyer had not articulated a proper legal basis for his request. (R.53). Beyer

responded via correspondence dated January 15, 2019, asserting both that due process required the requested disclosures and that the trial court had the authority to order the State to comply with the request under Wis. Stat. § 971.23. (R.54). Essentially, he argued that he was entitled to the discovery necessary to ascertain the validity of the allegations contained in the search warrant. (R.54). Beyer specifically invoked his right to put on a "complete" defense and contended that he had demonstrated the requisite "materiality" so as to compel the disclosures that he was requesting, citing *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), and *United States v. Ganias*, 824 F.3d 199 (2nd Cir. 2016) to support his position. (R.54).

On January 22, 2019, the trial court held a motion hearing on the discovery dispute. (R.95). The State argued that there was no statutory basis for Beyer's request on the grounds that it did not intend to introduce any evidence pertaining to the allegedly detected file at trial. (R.95:6-13). Beyer argued otherwise, analogizing the situation to cases involving drug detection dogs, asserting that he would have a right to inspect a given dog's records in order to interrogate the reliability of a given sniff or alert. (R.95:13-15). The trial court ultimately denied Beyer's motion, finding that Wis. Stat. § 971.23 did not require the disclosure of evidence that the State was not going to use at trial. (R.95:24-25; A:2-3). However, the trial court invited Beyer to file a suppression motion, at which juncture he would be permitted to cross-examine the law enforcement officers involved in preparing the application for the search warrant and to offer testimony through his own experts in support of a challenge to the warrant's validity. (R.95:24-25; A:2-3).

Beyer subsequently filed a "Motion to Suppress" on March 15, 2019, asserting that "(1) the search warrant lacked

probable cause in and of itself; (2) the agents relying on the search warrant knew that the search warrant lacked probable cause; and (3) the agents omitted and provided misleading information concerning its undercover investigative software (UIS)." (R.57:1). More pointedly, Beyer argued that the warrant offered very little from which to conclude that he knowingly possessed child pornography, noting the lack of information specific to Beyer vis-à-vis the "collectors" of child pornography described in the application's boilerplate or any information detailing his supposed interaction with the file detected by the UIS. (R.57:3-7). In other words, Beyer contended that extrapolation of probable cause from the alleged detection of a single—presently non-existent—file was unreasonable. On balance, he argued that the respective misrepresentations and omissions were tantamount to violation of *Franks v. Delaware*, 438 U.S. 154 (1978), and that the supporting affidavit was otherwise so substantively deficient that the "good faith" exception should not apply. (R.57:8-13). He also renewed his request to forensically analyze the State's UIS system, referencing a number of studies detailing the susceptibility of file sharing networks, and specifically BitTorrent, to malware and malicious digital file manipulation. (R.57:12-13;42-57).

The trial court held a hearing on Beyer's motion on March 22, 2019. (R.66). Special Agent Lenzner testified that in this case, the State utilized Torrential Downpour or Torrential Downpour Receptor, a computer program designed to identify users of the BitTorrent P2P network that are "sharing info hashes containing child pornography." (R.66:13-17). He explained that an info hash could contain one file or "thousands of files" and that "[t]here is a database of info hashes of child pornography uploaded in the software, and it automatically

detects when they're being shared on the BitTorrent network." (R.66:16-17). He stated that he received an alert about a file around October 28, 2017, and noted that the Torrential Downpour program had completed a single-source download of the file. (R.66:17-18; 22). He viewed the contents of the file, a video, and determined that it constituted child pornography. (R.66:17-18; 21-22). He then wrote an administrative subpoena for the IP address after determining that the internet service provider ("ISP") was Charter Communications/Spectrum using an ISP database. (R.66:19-20). The information provided by Charter identified Beyer as the subscriber for the relevant IP address. (R.66:19-20).

Agent Lenzner acknowledged that the file he purportedly viewed before drafting the administrative subpoena was not found on any of Beyer's electronic devices seized in the course of the execution of the search warrant. (R.66:22). When queried for an explanation, he stated

> [f]rom the date of the download, I believe it was October 28th, and the date of the warrant, I believe it was in December, there was a gap there where the party could have deleted the image. I don't know what happened to the image after it was downloaded or where it went, but to the best of my knowledge, I believe it was probably deleted. (R.66:23).

The State proceeded to ask, with respect to P2P cases specifically, "how common is it for you not being able to find the image later on?" (R.66:23). Agent Lenzner replied:

> [t]here's been a majority of cases where we went to do the search warrant—so, the time from we get [*sic*] the download to the time we do the warrant, between that time frame, the sooner we do it, the more likelihood we're going to find that file, but if we're doing search warrants 30 days, 60 days, 90 days down the road and they happen to delete that file or do something with that file, then it's more likely we're not going to find it. (R.66:23).

The State then inquired about "the normal practice that you've found" with respect to the tendencies of viewers of child pornography to save or delete files, to which Lenzner responded:

> [e]very target we deal with is different. Some people will keep that in a downloads folder. They'll download it, go back and view it later. After they view it, they will save it somewhere else. They'll delete it. Some people watch it right away and after watching, delete it. Sometimes they'll back it up on other devices to watch later. They'll categorize. Every person we deal with has a different way they categorize or do something with it after they download it. (R.66:23-24).

At that point, the trial court interjected:

> [l]et me just interrupt. I thought in the affidavit for the search warrant you both attested to the fact that they don't delete these things, that they keep them, and that's why you had reason to believe that there would be this image and others on his computer. Can you explain the apparent incongruity here? (R.66:24).

Lenzner replied:

> [c]orrect. So we deal with different types of offenders, or multiple different types, but the most common we deal with is we have collectors, and we have the people that are going to view right away and delete it. So we never know what kind of offender we're going to have at the time of the warrant. (R.66:24).

The trial court pressed Lenzner, stating, "[y]eah. You didn't mention that in the affidavit though. Why did you keep that out?" (R.66:25). Lenzner explained:

> I mean, we put the collector portion in there because when people do download files, people back up their stuff, whether they back it up on another hard drive or whatever they do with it, and people that are going to collect it and don't want family members or people living with them to find it or whatever the circumstances will take that and move it to another location. But not every single target we deal with is a collector, but there's a high likelihood that they are. (R.66:25).

On cross-examination, Lenzner admitted that the "collector" language at paragraph 22 of the warrant application was included in every search warrant application filed in these types of investigations, even though he acknowledged that there were actually "two different types" of offenders— "collectors" and "movers or storers"—and that he "did not know [Beyer] was a collector" at the time he viewed the file purportedly downloaded from a device at Beyer's IP address. (R.66:26-27). He also stated that he did not know how the file may have come

to be on Beyer's computer or whether Beyer ever actually viewed the file. (R.66:27-28).

In addition, Lenzner conceded that once he obtained a P2P user ID through the UIS, the State could conceivably utilize that information to track what that user was doing on the network and attempt to glean other incriminating, corroborative evidence from the user's shared files. (R.66:29-30).[2] He indicated that an IP address merely pertained to the "access point" or "modem" at Beyer's residence, and that any person who had access to the internet through that access point would share that IP address so the UIS-detected activity emanating from that address could not be contemporaneously traced to a specific device. (R.66:31-32).

Ultimately, Lenzner admitted that the only ways to establish whether the file mentioned in the search warrant application existed as alleged were through his testimony or by viewing his computer system and file logs for forensic verification. (R.66:32-33). He conceded that both the UIS and Beyer's P2P client were subject to malware, though he stated that he was not aware of having experienced an "infection" or discernible malfunction on his end. (R.66:33-36).

Following Lenzner's testimony, one of Beyer's forensic experts, Nicholas Schiavo, opined that the fact of the missing file signaled that it either never existed on Beyer's computer or

---

[2] At trial on August 30, 2022, Lenzner indicated that, "if that computer is sharing a known child–known file of child pornography, we could reconnect to that computer again and we could set our program to connect to that IP address when it's publicly sharing child pornography again." (R.175:18).

that it was manually deleted and overwritten, contrary to the typical behavior of viewers as described in the warrant application. (R.66:37-40). He stated that he believed it would be possible to verify that the file was present in Beyer's shared folder at the date and time in question through a forensic analysis of the State's system. (R.66:40). He also explained that a BitTorrent user could unwittingly receive and/or share illicit material by virtue of the program's dynamics: once a user requested a file and began a download, the user automatically began sharing that file even before the user conceivably has the ability to discern whether the file that was received was indeed what the user requested. (R.66:40-41). Schiavo further opined that a given IP address only identifies an internet router, and that any computer connected to the internet and P2P network via that router could have shared any given file traced to that address. (R.66:44).

Finally, Schiavo testified that uTorrent, the BitTorrent derivative that Beyer was alleged to have been using, had a documented programming flaw that "allowed it to be exploited by any user with a web browser." (R.66:45). More specifically, he stated that

> [a]nybody that was aware of the exploit could go back to anybody sharing a file and see anywhere on their computer, add files, subtract files, delete files, move them around, and it would appear as if it all happened in the shared folder because the way it works is it allows the bad actor to designate anywhere on the computer as the shared folder and look around and then manipulate it. (R.66:45).

When asked by the trial court whether he could establish that the exploit had been employed or abused in Beyer's case, Schiavo

explained that the missing file gave him "pause," but he could not do so definitively

> [w]ithout seeing the State's computer or knowing if they used the exploit or seeing logs from the State's computer that could tell me what the contents of the shared folder were over a period of time—for instance, if they changed dramatically, that would most likely mean from second to second that they're looking at a different folder but the system is still saying that it's the shared folder. (R.66:46-48).

On cross-examination, Schiavo went on to specifically explain that he could test whether a given exploit was abused by placing benign files in various places on a computer and then attempting to access those files over the torrent network with the State's computer. (R.66:54-55). At the close of testimony, Schiavo's colleague, Juanluis Villegas testified that out of over one-hundred child pornography investigations in which he had been involved, the file alleged to have been seen in order to get the search warrant was only charged once or twice. (R.66:62-64). He further testified that on approximately fifty-percent of the occasions where said file was not specifically charged, the file was never recovered. (R.66:64-65).

In argument, the State conceded that the warrant application "could be expanded greatly" but maintained that it still established probable cause by virtue of Agent Lenzner's testimony about the UIS system and his attestation to its reliability. (R.66:66-70; A:9-13). The State asserted that the fact of the missing file was irrelevant to the matter at hand and that Beyer's experts had failed to establish anything more than potential alternate possibilities as to how the file came to be

detected by the UIS and subsequently disappeared. (R.66:68; 71-75; A:11, 14-18).

While the State was dismissive of the idea that Beyer had established a *Franks* violation, the trial court noted that, with respect to evaluating past warrants of a similar nature, "I wish I would have known all this other information that came out today. Some of the issues, that folks in fact don't always save these and there's a high percentage of folks that delete them." (R.66:66; A:9). It went on to challenge the notion that Beyer had not shown that the application "omitted important factors that the court would have considered prior to issuing this," stating that "[b]oilerplate language is fine as long as it's true. Here the other side of the equation regarding the malware and regarding the other people's access to the computers and some people, a high number of people, delete the information, that would have been helpful, I think, to Judge Hyland, as it would be to me, in evaluating these." (R.66:70-71; A:13-14). In that same vein, the trial court observed that it

> almost seems directly implied from the affidavit that the defendant, based upon one image, this one video, was a collector, and all the assertions that follow that were that collectors save them, collectors distribute them, collectors do these things, but there's not any indicia at all that he's a collector from that one piece of evidence, and that seems to be coming up short in terms of the veracity of the affidavit. (R.66:71; A:14).

The court went on to note that "we've got an affiant who affirms or attests that this system that's being used is reliable, but there's no way to prove that" and that the affiant had "also candidly conceded that there is [*sic*] a lot of weaknesses that

would tend to detract from any belief in its reliability...[m]uch like...a confidential informant that in the past has come up with bad info." (R.66:73-74; A:16-17).

In spite of these observations, the trial court ultimately decided that there was a reasonable likelihood that the detected file could be found upon execution of the search warrant and that it was reasonable to believe that Beyer was the party who would be in possession of it, as "[t]he mere presence in his file on his computer I think is sufficient...for that purpose." (R.66:79-83; A:22-26). While declaring that the affidavits that accompany these warrants were cause for "a great deal of concern" and need "to be more individually tailored" with "more candid assessments of the reliability of this method of a search," the trial court concluded "that there was probable cause based upon the search warrant that was presented and that the officers had a right to execute that based upon the manner and form it was presented," thereby denying Beyer's motion in "a very, very close call." (R.66:82-83; A:25-26). A final order for the purpose of appeal was signed by the trial court on April 1, 2019. (R.65; A:28).

On April 17, 2019, Beyer filed a Motion for Reconsideration of the court's decision to deny its request to inspect the State's UIS. (R.67). The trial court ultimately denied this motion on May 20, 2019. (R.70; A:29-30).

On June 13, 2019, the trial court found Beyer guilty on Count 1 of the Information based upon a stipulation after his waiver of a jury trial. (R.93; A:31). The State moved to dismiss Counts 2-10. (R.93:A:31). The court subsequently sentenced Beyer to three years of initial confinement and two years of extended supervision, but stayed the sentence pending appeal. (R.85; A:53). Beyer filed a Notice of Intent to Seek Post-

Conviction Relief on July 24, 2019 (R.88), and a Notice of Appeal on October 15, 2019. (R.99).

In its appellate brief the State asserted that the court trial was not a trial but actually tantamount to a guilty plea used to circumvent the guilty plea waiver rule in order for Beyer to be able to appeal the denial of his discovery motion. The Court of Appeals certified the matter regarding the validity of the court trial to the Supreme Court. (R.136:13-14; A:67-68).

The Supreme Court rendered its decision on June 15, 2021, and held that the activity in the trial court was neither a guilty plea nor a court trial (R.138:15-16; A:84-85). It remanded the case to the trial court and allowed Beyer to either plead guilty to the original count or withdraw his plea and proceed to trial. (R.138:15-16; A:84-85).

Following a denial of his second motion to reconsider the original trial court denial of his motion to suppress, Beyer subsequently proceeded to a court trial on August 30, 2022. (R. 150; R.175; A:87-88; A:89). Originally, the State attempted to reinstate all ten charges in the original complaint after having dismissed nine of the ten charges at the time of the first trial on June 13, 2019. Beyer objected by written motion and the State ultimately agreed to proceed to trial on Count 1 of the original complaint only. (R.146-147,149).

At the trial the State presented four witnesses: agent Lenzer, a lieutenant involved in drafting the search warrant; the detective, Scott Sachtjen, who interviewed Beyer at the scene of the execution of the search warrant; and the DCI computer analyst, Stacey Sadoff.

Sadoff's testimony provided the basis for Beyer's defense. While in a van at the search warrant scene, she analyzed Beyer's electronic device after it was seized during the

execution of the warrant. (R.175:33; A:97). She discovered child pornography on his hard drive during her examination. Each file she documented contained the time the file was created (when the file first came onto his device), the time it was last accessed (the time he last would have viewed it), and the time the file was modified (if/when it was altered). (R.175:37-38; A:101-102). The images contained in counts one through 6 all arrived on Beyer's device within 26 seconds of one another. (R175:45; A:109). They were all from a series labeled "Siberian Mouse." Beyer was on a file sharing network which allowed him to share files from his computer with others and others to share files with him. If he clicked on "Siberian Mouse" it is unclear if he knew the images he was going to receive contained child pornography. (R.175:45-46; A:109-110). Sadoff testified that she could not tell whether Beyer knew the images from Siberian Mouse were on his computer. (R.175:45-46; A:109-110).

Images 2-6 in the Siberian Mouse series had different dates for "Last accessed" and "Entry modified." Count 1 however, the charge for which he was on trial, did not have different dates for "Last accessed" or "Entry modified." (R.175:39-41,43-46; A:103-105). That is why Sadoff could not determine whether Beyer ever knew the image in Count 1 was even on his computer. Because there was no proof Beyer even knew the image from Count 1 was on his device, Beyer asserted that he could not have knowingly possessed it, nor could the State prove he knew what the image contained. Accordingly, he argued that the State had not proven him guilty beyond a reasonable doubt of knowingly possessing the image depicted in count 1.(R.175:88-90; A:113-115). The trial court disagreed, finding that there was circumstantial evidence to support that the

specific image concerned was viewed by Beyer beyond a reasonable doubt—namely "[t]he fact that the other images [were] in the same location and certainly they were viewed." (R.175:96-97; R.199:1-2; A:118-119; A:125-126).

## ARGUMENT

Beyer made two essential contentions in his initial appeal: (1) the denial of his request to forensically examine the State's computer and UIS constituted a denial of his right to due process; and (2) the trial court erred in denying his motion to suppress on the grounds that the warrant application failed to establish probable cause. He now asserts in addition to these arguments that (3) there was insufficient evidence from which the trial court in the second trial could find him guilty beyond a reasonable doubt on the count for which he was retried.

## STANDARD OF REVIEW

Discovery decisions by the trial court are generally governed by a discretionary standard of review. *State v. O'Brien*, 214 Wis. 2d 328, 344, 572 N.W.2d 870, 877-78 (Ct. App. 1997), aff'd, 223 Wis. 2d 303, 588 N.W.2d 8 (1999). However, constitutional questions are subject to *de novo* review. *State v. Schaefer*, 2008 WI 25, ¶ 17, 308 Wis.2d 279, 746 N.W.2d 45. Accordingly, appellate courts review the underlying historical facts under the clearly erroneous standard but review questions of ultimate constitutional fact independently. See *State v. Harris*, 2004 WI 64, ¶ 11, 272 Wis. 2d 80, 94, 680 N.W.2d 737, 745.

A two-part standard of review applies in reviewing a denial of a motion to suppress: the trial court's findings of fact shall be upheld unless they are clearly erroneous, but whether those facts warrant suppression and whether the trial court properly applied constitutional principles to those facts is subject to *de novo* review. *State v. Conner*, 2012 WI App 105, ¶ 15, 344 Wis. 2d 233, 243, 821 N.W.2d 267, 271; *State v. Smiter*, 2011 WI App 15, ¶ 9, 331 Wis. 2d 431, 436, 793 N.W.2d 920, 922.

An appellate court considers the totality of the evidence when reviewing the sufficiency of the evidence to support a conviction. *State v. Coughlin,* 2022 WI 43¶ 24,25, 402 Wis 2d. 107, 118,119. Deference is given to the jury (finder of fact) determination of guilt and the evidence is viewed in the light most favorable to the State. *Id.*

## I. THE DEPRIVATION OF AN OPPORTUNITY TO FORENSICALLY EXAMINE THE STATE'S COMPUTER SYSTEM AND UIS CONSTITUTED A VIOLATION OF BEYER'S DUE PROCESS RIGHTS.

The right of an accused to present a defense is fundamental and is embodied in the due process guarantees of the Fifth, Sixth, and Fourteenth Amendments of the United States Constitution. *State v. Schaefer*, 2008 WI 25, 20, 308 Wis. 2d 279, 291, 746 N.W.2d 457, 463 (*citing Washington v. Texas*, 388 U.S. 14, 19, 87 S.Ct. 1920, 18 L.Ed.2d 1019 (1967)). "Due process preserves an accused's right to challenge the prosecution's case by obtaining evidence tending to establish the

accused's innocence or by casting doubt upon the persuasiveness of the prosecution's evidence." *Id.*

The broad right to pretrial discovery, as it directly "concerns the ultimate ability of a defendant to present relevant evidence and witnesses in defense of criminal charge," is an essential element of due process. *State v. Maday*, 179 Wis. 2d 346, 354, 507 N.W.2d 365, 369 (Ct. App. 1993). Ultimately, "pretrial discovery" signifies the defendant's fundamental "right" to "obtain evidence necessary to prepare his or her case for trial. *Id.* Discovery should be more than a mere perfunctory exercise, as "providing a defendant with meaningful pretrial discovery underwrites the interest of the state in guaranteeing that the quest for the truth will happen during a fair trial." *Id.* Fundamental fairness requires "that criminal defendants be afforded a meaningful opportunity to present a complete defense," which is safeguarded by "constitutionally guaranteed access to evidence."*California v. Trombetta*, 467 U.S. 479, 485, 104 S. Ct. 2528, 2532, 81 L. Ed. 2d 413 (1984)(citing *United States v. Valenzuela–Bernal*, 458 U.S. 858, 867, 102 S.Ct. 3440, 3447, 73 L.Ed.2d 1193 (1982)).

Even though Beyer acknowledges that the disclosures he sought did not directly concern evidence that the State intended to introduce at trial, he believes that "pretrial discovery" prescriptions outlined above remain applicable given the intersection of rights and procedure at which this controversy arises. At least some courts have expressly held that "the failure to disclose information material to a ruling on a Fourth Amendment suppression motion can constitute a *Brady* violation," suggesting that the mere fact that the State does not intend to produce warrant-initiating evidence at trial in the context presented here is not dispositive on the issue of whether

discovery regarding the means by which that evidence was purportedly procured is either permissible or required. See *Biles v. United States*, 101 A.3d 1012 (D.C. App. 2014). Thus, the question as to whether a defendant is constitutionally entitled to the disclosures sought in this specific context appears to be unsettled— Beyer is not aware of any reportable decisions on this acute discovery issue in the State of Wisconsin.

However, for guidance—and in tracking the logic of this Court's per curiam discussion of a similar situation in *State v. Lovell*, 2019 WI App 33, ¶ 27, 388 Wis. 2d 144, 930 N.W.2d 276— Beyer would look to the body of case law outlining the general obligation of the State to disclose evidence that is "material to guilt or innocence." *State v. Harris*, 2004 WI 64, ¶ 12, 272 Wis. 2d 80, 94–95, 680 N.W.2d 737, 745. In this context, the derivative implication of that general guiding principle as to necessary disclosures would be that a defendant seeking "due process" disclosure of pretrial discovery not specifically mandated by Wis. Stat. § 971.23 needs to establish the materiality of that discovery to a specific proceeding. More specifically, a defendant in Beyer's situation would need to demonstrate materiality by proffering information sufficient to establish a "reasonable probability" that had the evidence been disclosed, the result of his suppression hearing would have been different. *United States v. Bagley*, 473 U.S. 667, 682, 105 S. Ct. 3375, 3383, 87 L. Ed. 2d 481 (1985) In contrast with the situation presented in *Lovell*, where the defendant was deemed to have largely relied only upon speculative reasoning, Beyer believes that the record here staunchly supports the notion that the disclosure of the evidence he seeks was reasonably likely to change the result of his suppression motion.

Here, Beyer introduced expert testimony that specifically delineated a well-documented Torrent-specific system susceptibility that was available for exploitation at the time of concern. (R.66:37-40). Beyer's expert also stated the precise manner by which the exploit could be utilized to manipulate files on the Torrent network which, in conjunction with the "indirect evidence" of the missing file, offered a coherent explanation as to how the file that the State claims to have detected seems to have briefly appeared and then disappeared by either malfeasance or malfunction. (R.66:40-41;45-48). Finally, his expert also explained the discrete types of tests he could run to interrogate the data in a fairly straightforward procedure. (R.66:54-55).

In other words, Beyer did not lay the groundwork for a speculative expedition: he specifically explained how the particularized dynamics of the P2P network at issue raised serious questions as to the reliability of the UIS detection in this case which was also called into question by the fact of the missing file of import. The State's expert conceded an awareness of the potential susceptibilities of the program, but he was admittedly not a computer forensic analyst and could not offer a great deal of clarity regarding the nuances of the system upon which Beyer's expert homed in. (R.66:32-36). In essence, Agent Lenzner's testimony simply boiled down to the bare assertion that the UIS had been successful in detecting illicit files in the past and he therefore assumed it was reliable in this case. He offered nothing else to rebut Beyer's expert.

Beyer would submit that, in light of the issues raised by his experts, to effectively render the Agent's testimony as to the reliability of the UIS as the unimpeachable final word on the matter would be incompatible with due process. To allow the

State to avoid making the sought disclosure—where the warrant only alleged the detection of a single file that was never recovered and where forensic experts have pointed to specific programming flaws that are reasonably likely to explain that occurrence—would be to set the bar for "materiality" unduly high. More importantly, it would also effectively signal that the State is afforded carte blanche via rubber-stamped warrants to search the homes and electronic devices of its citizenry for any manner of pursuits and propelled by whatever sort of motivation so long as it simply alleges that its UIS made a detection of a single illicit file at an IP address for which any given individual foots the bill. As it stands, the State is afforded free rein to make the absolute bare minimum allegation in order to acquire approval for a broader search with full-confidence that its inscrutable processes and procedures will avoid any scrutiny whatsoever—assuming that some sort of independently incriminating evidence is discovered thereafter—so long as it elects not to base any criminal prosecution on whatever illicit material that it alleged to have detected in order to have the search endorsed in the first place. Beyer submits that this is entirely irreconcilable with the spirit of the Fourth Amendment and any reasonable understanding of what "due process" entails.

Though Wisconsin precedent in this specific area is again lacking, Beyer has identified a few federal cases which he believes are instructive as to the means by which a defendant might establish the requisite level of materiality to a constitutionally-implicative pretrial proceeding so as to warrant the sort of disclosures he seeks. In *United States v. Budziak*, 697 F.3d 1105, 1112-13 (9th Cir. 2012), the defendant filed three motions to compel discovery, asking for access to the UIS program and its technical specifications after presenting

evidence that suggested that the UIS of concern could potentially override "shared" folder settings. Given that showing, the Court found that district courts "should not merely defer to government assertions that discovery would be fruitless." *Id.* at 1113. More specifically, it concluded that "[i]n cases where the defendant has demonstrated materiality," and where "the charge against the defendant is predicated largely on computer software functioning in the manner described by the Government and the Government is the only party with access to that software," it is an abuse of discretion for a trial court to deny the defendant discovery of the program. *Id.* As for the manner by which Budziak had demonstrated materiality, the court explained "[a]ll three of Budziak's motions to compel provided more than a general description of the information sought; they specifically requested disclosure of the EP2P program and its technical specifications" and that he had identified specific defenses that the sought discovery "could potentially help him develop." *Id.* at 1112.

Noting how the denied discovery hamstrung Budziak's potential defense, the court found that he had been denied "background material" that could have enabled him to pursue a more effective [cross] examination of the government's UIS expert, and reaffirmed that

> "[a] party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately." *United States v. Liebert*, 519 F.2d 542, 547–48 (3d Cir.1975).

*Id.*[3]

In *United States v. Gonzales*, No. CR1701311001PHXDGC, 2019 WL 669813 (D. Ariz. Feb. 19, 2019), the Government's UIS, Torrential Downpour, was patrolling BitTorrent P2P networks just as the State's UIS was in Beyer's case. The BitTorrent UIS searched the network for IP addresses offering torrents containing known child pornography files. *Id.* at *1-2. A law enforcement agent used Torrential Downpour to identify an IP address which allegedly was making known child pornography files available on the Bit Torrent network. *Id.* He reviewed the activity logs to confirm that the program downloaded complete files solely from this IP address and then reviewed the video files to confirm that they were, in fact, child pornography. *Id.* Two months later, he sought and obtained a search warrant which resulted in the discovery of various images of child pornography on a tablet device. *Id.*

---

3

The reasoning in *Budziak* was used by the District Court in *United States v. Crowe,* 2013WL12335320, to grant the defendant's motion to allow his forensic expert to conduct an independent examination of the UIS used to allegedly locate hash values related to child pornography from a file sharing network used by the defendant. There the files alleged to have been found by law enforcement while using its UIS in the shared space on Crowe's computer were not found during the defense expert's analysis just as the one file alleged to have been seen by the DCI agent in Beyer's case was never located after the execution of the search warrant. From this fact alone, the Court concluded that Crowe was entitled to test the reliability of the computer evidence used against him.

Defendant Gonzales contended that the UIS may be flawed and should be tested and verified by a third party. He sought disclosure of an installable copy of the software pursuant to Rule 16 of the Federal Rules of Criminal Procedure, *Brady v. Maryland, 373 U.S.* 83, 83 S.Ct. 1194, 10 L.Ed.2d 215 (1963), *Giglio v. United States*, 405 U.S. 150, 92 S.Ct. 763, 31 L.Ed.2d 104 (1972), and their progeny, which generally dictate that the Government must turn over items that are material to preparing a defense. *Id.* at *4-5. He relied on *Budziak* to support his position, and introduced expert testimony stating "that all of these programs 'contain bugs, they do not always function as intended and the data reported by these applications is not always accurate or reliable.'" *Id.* at *4. The court ultimately found that Gonzales' expert established materiality of the disclosures by virtue of her having

> provided a plausible explanation for how Torrential Downpour may have erroneously identified Gonzales's tablet as offering child pornography files over the BitTorrent network... She further stated that a forensic examination of the device used to download the torrent can determine whether the torrent has been used to download the file, and her examination of Gonzales's tablet revealed no evidence suggesting that he downloaded the files listed in counts one through eight. She opined that Torrential Downpour may have obtained the files from other BitTorrent users, particularly in light of the fact that this is how peer-to-peer file sharing programs are designed to work.

*Id.* at *5.

In light of that showing of materiality, and referring to *Budziak*, the *Gonzales* court indicated that Gonzales should be

given access to the Government's program to investigate its reliability and help him prepare for cross-examination. *Id.* at *6.

Finally, in *United States v. Owens*, No. 18-CR-157, 2019 WL 6896144 (E.D. Wis. Dec. 18, 2019), the Eastern District of Wisconsin had occasion to review a case touching upon many of the same issues. Following a BitTorrent investigation wherein Torrential Downpour Receptor allegedly detected a single video file of child pornography at an IP address traced to the defendant, a search warrant was executed. *Id.* at *1. Law enforcement was unable to locate the video file that was allegedly detected. *Id.* The defendant sought disclosure of the UIS largely based on this discrepancy and expert testimony that "a universal truth about computer software is that there are always bugs, errors, or malfunctions in it." *Id.* at *4. The court found that such generalized, conclusory offerings did not meet the materiality standard, and more importantly, it seems that the State's expert was actually able

> to point to evidence on Owens' computer showing that the child pornography files downloaded by law enforcement using TDR had been on his computer at the time of the downloads and thus must have been deleted sometime before the search warrant on his home was executed and his computer seized.

*Id.*

In Beyer's case, the defense expert testimony coupled with the missing file was far more developed and specific with respect to the computer systems at issue. Moreover, there was no secondary demonstration by law enforcement using any computer that the file allegedly downloaded by the UIS was present on Beyer's device at the time of the alleged download.

Frankly, since that is something that law enforcement is apparently capable of demonstrating without compromising sensitive information, the State's refusal to do so in Beyer's case seems all the more problematic given the prevailing rationale for continuing to give this enigmatic system the benefit of the doubt.

In sum, Beyer asserts that his due process rights obligate the State to disclose evidence of a violation of his Fourth Amendment rights and/or evidence that would be reasonably likely to change the course of a pretrial proceeding. He submits that he has made the requisite showing of materiality under the relevant precedential framework which should require the disclosures which he seeks. He asks this Court to find that the trial court erroneously declined to issue the appropriate discovery order and remand for further proceedings.

## II. THE WARRANT APPLICATION FAILED TO ESTABLISH PROBABLE CAUSE AND THEREFORE SUPPRESSION WAS WARRANTED.

The warrant clause of the Fourth Amendment requires that the government establish probable cause to justify the issuance of a warrant. *United States v. Rabe*, 848 F.2d 994, 996 (9th Cir. 1988). The issuing magistrate must be convinced that there is at least a fair probability that evidence of a crime will be found in the location targeted for a search. *Id.* Each case must be viewed on a case-by-case basis. *United States v. Prideaux-Wentz*, 543 F.3d 954, 958 (7th Cir. 2008). See also *State v. Gralinski*, 2007 WI App 233, 306 Wis.2d 101, 743 N.W.2d 448. Great deference is given to the warrant-issuing

judge's determination of probable cause, and that determination will stand unless a defendant establishes that the facts are clearly insufficient to support that finding. *State v. Multaler*, 2002 WI 35, ¶ 7, 252 Wis. 2d 54, 62, 643 N.W.2d 437, 441.

In this case, Beyer submits that the original search warrant was insufficient to support probable cause in and of itself. However, he also contends that a series of deliberate misrepresentations and omissions in the warrant application that were later established by testimony should have required the trial court to grant his motion to suppress under *Franks v. Delaware*, 438 U.S. 154, 154, 98 S. Ct. 2674, 2676, 57 L. Ed. 2d 667 (1978), and *State v. Mann*, 123 Wis. 2d 375, 387, 367 N.W.2d 209, 214 (1985).

### A. The warrant application failed to support probable cause on its face and the "good faith" exception should not apply.

In reviewing the search warrant application, Beyer contends that there was very little information from which to conclude that he likely knowingly possessed child pornography on an electronic device or that he met the criteria for someone who is likely to retain pornography as implied by the boilerplate language contained therein.

In the first instance, the application makes no indication as to how the single file it mentioned was linked to the cited IP address. There are no search terms noted in the warrant application which would suggest that Beyer was actively seeking to download child pornography onto his device. The application also offers nothing to indicate that Beyer ever viewed the file or

the duration of time that he may have viewed it.[4] There is no information whatsoever suggesting how he came to allegedly obtain the file or what, if anything, he did with it.

Furthermore, Wisconsin Criminal Jury Instruction 2146A describes the elements of the crime that the State must prove: first, "that the defendant knowingly either possessed a recording" or "accessed a recording in any way with intent to view it." "Possessed" means that "the defendant knowingly had actual physical control over the recording." Second, the jury instruction requires that the recording "showed a child engaged in sexually explicit conduct." Third, the State must prove that "the defendant knew or reasonably should have known that the recording contained depictions of a person engaged in actual or simulated" sexually explicit conduct. Finally, the State must prove that the defendant knew or reasonably should have known that the person shown in the recording engaged in sexually explicit conduct was under the age of 18 years. The warrant application simply does not come close to providing sufficient information to render it reasonable to believe that Beyer was engaged any of that proscribed type of behavior or that evidence thereof was likely to be recovered.

More critically, paragraph 22 of the warrant application specifically claimed that the purported tendency of individuals who have an interest in child pornography to retain any images or videos they obtain that depict such activity made it reasonably likely that illicit material could be recovered in Beyer's case. (R.55:17). However, nothing in the application was subsequently

[4]See footnote 1 above.

offered to confirm or corroborate that Beyer may be one of these people.

Beyer would submit that this conspicuous absence of information is highly troubling in light of the fact that during the approximately 40 days from the time the agent allegedly detected this single file of pornography to the time the search warrant was executed, the agent never returned to that IP address to see if any additional images could be found to help tailor the warrant application to Beyer as an individual. The State plainly had plenty of time to monitor Beyer in order to do so, as it had already identified a BitTorrent peer ID and logged an IP address. And yet, nothing in the warrant application was provided to evince Beyer's purported propensity to be a collector of child pornography or someone who was even interested in child pornography. The alleged proclivities of collectors of child pornography mentioned in the application would only seem to be relevant information if there was actually some established or intelligible reason to believe that Beyer was a collector. Here, there was no attestation with respect to some of the factors ostensible relevant to establishing such a belief: (1) whether he had been identified as a pedophile; (2) whether he had paid for access to child pornography web sites or memberships; (3) whether he had an extended history of possessing or receiving pornographic images; (4) whether it was a complicated process for him to obtain the images as opposed to simply having to click the mouse; and (5) whether there was any evidence that the he redistributed those files to others. *United States v. Raymonda*, 780 F.3d 105, 114–15 (2d Cir. 2015). The only information ostensibly offered to suggest that Beyer was a collector was the mere allegation that, on one particular day for approximately two minutes, there was a single file that a State agent claims he saw

on Mr. Beyer's computer a file which ultimately could not be found after the State seized the computer 40 days later. The application does not precisely denote how many images or pictures one must possess in order to be defined as a "collector," but presumably that figure is greater than one in the absence of any other tangible supporting evidence.[5]

Further, Beyer submits that it is well-settled law that a person's mere propinquity to others independently suspected of criminal activity does not, without more corroborative proof, give rise to probable cause to search that person. *Ybarra v. Illinois*, 444 U.S. 85, 91, 100 S. Ct. 338, 342, 62 L. Ed. 2d 238 (1979). The notion that the act of an agent seeing one image on a file-sharing network that may be used for illicit purposes provides probable cause for the police to enter an individual's private dwelling and rummage through his personal effects is utterly anathema to the Fourth Amendment. *Payton v. New York*, 445 U.S. 573, 585, 100 S. Ct. 1371, 1379, 63 L. Ed. 2d 639 (1980). To conclude that the slim evidence yielded from the

---

5 See *Raymonda*, 780 F.3d at 115, referring to a survey of federal cases where courts had inferred that a suspect was a collector on the basis of a single incident of possession or receipt:

> [i]n all of these cases, the inference that the suspect was a collector of child pornography did not proceed merely from evidence of his access to child pornography at a single time in the past. Rather, it proceeded from circumstances suggesting that he had accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection. Such circumstances tend to negate the possibility that a suspect's brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged.

State's minimal investigatory efforts provided reason to believe that child pornography could likely be recovered from Beyer's home required a number of inferential leaps of faith that were frankly unreasonable given the dearth of illuminating information in the warrant application. The application here was limited almost entirely to boilerplate recitations—it was imbued neither with facts immediately pertinent to this particular case nor details regarding this particular defendant. There was simply nothing offered to actually bolt Beyer to the boilerplate. In light of the sheer anemia of the application, Beyer submits that the facts are clearly insufficient to allow the issuing judge's determination of probable cause to stand.

Upon invalidating a search warrant that was issued without probable cause, a reviewing court needs to next assess whether the officers who executed the warrant relied in good faith on its validity to determine whether evidence obtained pursuant to the invalid warrant should be suppressed. *United States v. Leon*, 468 U.S. 897, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984). In Wisconsin, an exception to the exclusionary rule exists where police officers act in objectively reasonable reliance on the search warrant issued by a neutral and detached magistrate. *State v. Eason*, 2001 WI 98, ¶ 27, 245 Wis. 2d 206, 231, 629 N.W.2d 625, 635. Objectively reasonable reliance on a search warrant requires that the officers conduct a significant investigation prior to obtaining a warrant; that a knowledgeable police officer or government attorney review the warrant application; and that a reasonably well-trained police officer would not know the search was illegal despite the magistrate's authorization. *State v. Scull*, 2015 WI 22, ¶ 38, 361 Wis. 2d 288, 307, 862 N.W.2d 562, 571.

The objective standard requires officers to have a reasonable knowledge of what the law prohibits. *Leon*, 468 U.S. at 919. An officer does not manifest objective good faith in relying on a warrant based on an affidavit so lacking in indicia of probable cause that it would be entirely unreasonable to believe in its validity. An important consideration in determining whether law enforcement has demonstrated good faith is the time pressure under which the officer was operating when he prepared the warrant application: the rationale behind *Leon* being that since law enforcement officers are not lawyers they must often make hurried judgments and therefore some degree of latitude should be afforded. *Id.* at 914. In this case, the State dictated the manner and the method the investigation and had complete control over the timing of application for the search warrant, which—at least according to the affidavit—was not altogether that important to the likelihood of discovering the alleged contraband. Under those circumstances, where there was no purported exigency, law enforcement's conduct should not be condoned on the grounds of practical constraints. Beyer submits that the relevant representatives of law enforcement in his case were well-aware that they were tendering the sort of bare-bones application that is clearly deficient under *Leon* and its progeny, and that the good faith doctrine is therefore inapplicable.

B. The warrant application contained deliberately misleading information about offenders' propensity for collecting child pornography, recklessly implied that Beyer was a "collector" in the absence of any corroborative basis for doing so, and deliberately omitted relevant information material to a reviewing magistrate's evaluation of the reliability of the information provided via the State's UIS, rendering it invalid under *Franks/Mann*.

At the motion hearing on March 22, 2019, Agent Lenzner offered extensive testimony that largely contradicted the boilerplate representations in the warrant application that viewers of child pornographers tended to be "collectors" that retained contraband data and therefore made it reasonably likely that the illicit file detected by the UIS would be recovered through the execution of a search warrant. (R.66:22-25). He was candid, as the trial court observed, in admitting that a significant percentage of offenders were actually not collectors, and that the UIS-detected files were actually often not recoverable due to deletion or other reasons—though these acknowledged realities went entirely unmentioned in the warrant application. Lenzner also frankly conceded that he had no reason to believe that Beyer was a "collector" of child pornography based upon the detection of the single illicit file by the UIS. (R.66:26-28). Finally, his testimony made it abundantly clear that the passage of time was the more apt consideration in predicting the likelihood of recovering any given detected file of contraband, therein completely contradicting the significant portion of the application

devoted to establishing the propensity of offenders to "collect" as the key to the probable cause equation.

The trial court itself expressed extreme reservations regarding the obvious incongruity between Agent Lenzner's testimony and the information provided in the warrant application. It noted that it was specifically troubled by the misleading information about the tendencies of offenders, the undue insinuation that Beyer was an individual who shared such tendencies, and the testimony which suggested that the UIS had been unreliable on occasion in the past in terms of law enforcement's relative success rate in recovering the files that were allegedly detected, likening it to an undercover informant who had come up with "bad info" in the past. (R.66: 66,70-71, 73-74; A:9,13-14,16-17). Beyer submits that the trial court was absolutely correct to criticize all of these respective shortcomings, but ultimately erred in determining that they did not warrant suppression on aggregate pursuant to *Franks/Mann*.

*State v. Mann* dictates that "[i]n the *Franks* context of search warrants," the deliberate or reckless "misrepresentations of the affiant are removed from the search warrant application and if probable cause therefore does not exist independently, the effect and sanction is the exclusion of the seized evidence." 123 Wis. 2d 375, 387, 367 N.W.2d 209, 214 (1985). To prove "reckless disregard" for the truth, a defendant must show that the affiant in fact entertained serious doubts as to the truth of the allegations or had obvious reasons to doubt the veracity of the allegations." *State v. Anderson*, 138 Wis. 2d 451, 463, 406 N.W.2d 398, 404 (1987). A "material omission" should be accorded similar treatment in the reevaluation whether a warrant application developed probable cause if it "is a fact critical for a fair decision which is known by the state" and has been omitted.

*Mann*, 123 Wis.2d at 388. A court deciding whether an omission was material should consider whether it is the case that "if the fact were included, the affidavit would not support a finding of probable cause." *United States v. Williams*, 737 F.2d 594, 604 (7th Cir. 1984).

Here, Beyer submits that the misrepresentations about the expected tendencies of offenders, when coupled with the misrepresentation that there was reason to believe that Beyer fell into a certain category offender and the omission of critical information about the preeminence of temporal considerations in determining the likelihood of recovering detected contraband (which largely undermined the entire substantive foundation for the assertion that probable cause existed), should have had the effect of invalidating the search warrant. Agent Lenzner's own testimony made it clear that these were not innocent or negligent errors and omissions—these were representations that are included in every warrant application in spite of their known inaccuracies or inapplicability because, unchallenged and uninterrogated, they improve the likelihood of warrant endorsement where the incriminating evidence that is specific to a particular defendant is minimal in the extreme, as was the case here. If the detection of a single file renders an individual an offender, and every offender is categorized as a collector—thereby rendering other ostensibly significant considerations effectively irrelevant—then a finding of probable cause in the context of a warrant application is more or less an absolute certainty. So although the trial court may have lamented a lack of much-needed "tailoring" of the application here in reference to Beyer, the real fact of the matter is that this application was fashioned quite precisely with the express purpose of flattering a breathtaking thinness.

In sum, Beyer submits that Agent Lenzner's testimony demonstrated a clear awareness that much of the warrant boilerplate referring to collectors and the likelihood of recovering evidence after only a relatively short amount of time had passed was tremendously misleading at best, if not outdated in general and outright fictive as applied to him.[6] In light of that, Beyer would submit that the trial court's finding that there was no misconduct on Lenzner's part which would warrant application of the exclusionary rule for its deterrent effect on his part was clearly erroneous and demands rectification on appeal. Furthermore, Beyer would submit that once the misrepresentations and distortions in the warrant are either removed or (dis)qualified by Agent Lenzner's own testimony, the allegation that a single illicit file was detected at IP address associated with him forty days prior cannot reasonably support a finding of probable cause so as to validate the search warrant.

## III. THERE WAS INSUFFICIENT EVIDENCE TO SUPPORT A CONVICTION FOR ONE COUNT OF POSSESSION OF CHILD PORNOGRAPHY AT THE COURT TRIAL ON AUGUST 30, 2022.

---

6 See *United States v. Clark*, 668 F.3d 934, 939 (7th Cir. 2012): "[b]oilerplate language about the tendencies of child pornography collectors supports probable cause for a search when the affidavit also includes facts that suggest the target of the search 'has the characteristics of a prototypical child pornography collector.'"

In determining whether there is sufficient evidence to support a conviction, the appellate court considers the totality of the evidence. *State v. Coughlin*, 402 Wis. 2d 107, 119, 975 N.W 2d 179, 185(2022). This should be evaluated according to jury instructions rather than verdict forms. *Id.* The appellate court may not substitute its opinion of the evidence unless after viewing the evidence in the light most favorable to the state, the evidence is so lacking in probative value and force that no trier of fact could reasonably find guilt beyond a reasonable doubt. *State v. Poellinger*, 153 Wis. 3d 493, 507, 451 N.W. 2d 752(1990).

After the remand from the Supreme Court, the state wanted to reinstate counts 2-10 which the state had dismissed at the time of the first trial. Beyer objected (R.146), and filed a memorandum in support of his position.(R.147). The state agreed that it would not refile those charges that were dismissed earlier.(R.149). Therefore, the only issue in the second court trial was whether Beyer knowingly possessed child pornography as it related to count 1 in the original information.

Jury instruction 2146A lists the elements that need to be proved to convict someone of possession of child pornography.(See page 21, supra). To knowingly possess something one would presume the person had to first see its contents. Without seeing it, it would be impossible to know the age of the person depicted in the image and whether that person was engaged in a sexual act.

The parties proceeded to have a second court trial on August 30, 2022. The state called four witnesses including Agent Lenzner, DCI analyst Stacey Sadoff, and Detective Scott Sachtjen who interviewd Beyer at the time of the arrest warrant. Beyer admitted to Sachtjen that he had a file sharing network and he had downloaded child pornography from that

network.(R.175:59). However Beyer argued that the issue was not that he downloaded other child pornography but whether he knowingly possessed the child pornography depicted in count 1 of the information.(R.175:64-65). On cross examination, Sachtjen admitted that Beyer told him that when he went on the file sharing network, he sometimes received things that he was not expecting. (R175:77). No search terms which would typically be used to search for child pornography were found on his devices.(R.175:45,77).

Sadoff the DCI analyst testified that Beyer's computer automatically tracked certain details about each image that came onto his computer. The first detail that was tracked "file created," which is defined as the date and time the specific image came onto Beyer's hard drive.(R.175:43; A:107). In this case six images all came onto his hard drive on September 9, at 12:26:41 within 26 seconds UTC. (R.175:45; A:109). The second detail tracked is "last accessed", which is the last time someone physically looked at the image.(R.175:44; A:108). The last detail tracked is "entry modified", which is when the image was altered by someone viewing it. (R.175:46; A:110).

When the images were downloaded onto Beyer's device they came in very quickly and Sachtjen stated they were in thumbnail form meaning many images were on one screen and they were very small. (R.175:78; A:110-11).

Sadoff testified that she could not tell whether Beyer even knew the image in count 1 of the information was on his computer, because the file created, last accessed and entry modified never changed from the time the image came onto his hard drive.(R.175:46-47).

The issue for the court to decide was whether Beyer knowingly possessed the image depicted in count 1 of the

information, not whether there were other images of child pornography on his computer. If there was no proof that Beyer ever saw the specific image of concern, how could he possibly knowingly possess it? How could he have known that the child depicted in said image was under 18 if he never saw the image? How could he know a child was engaged in sexual activity if he never saw the image?

Beyer admitted he had child pornography on his computer, but that was not the issue for this court to decide. The issue was whether Beyer knowingly possessed the specific image referenced in count 1. Since there was no proof he ever saw that image, he submits that the State did not prove him guilty beyond a reasonable doubt of knowingly possessing child pornography as it relates to the charged image and urges this Court to find the State did not meet its burden of proof and reverse the conviction in this case.

## CONCLUSION

For all of the foregoing reasons, Beyer respectfully asks this Court to find that the decision to deny his request to inspect and analyze the computer system purportedly employed by the State to detect the single file of child pornography comprising the fundamental basis for the issuance of the search warrant in this case was constitutionally infirm and otherwise denied him due process. Next, he asks this Court to find that the evidentiary fruits yielded through the execution of the search warrant should be suppressed on the grounds that the affidavit in support of said warrant failed to establish probable cause. Finally, and/or in the alternative, he asks the Court to find that the State failed to prove him guilty beyond a reasonable doubt of knowingly possessing child pornography as it relates to count 1 of the information.

Dated this 13 day of March, 2023.

EISENBERG LAW OFFICES, S.C.

Mark A. Eisenberg
State Bar Number: 1013078
308 E. Washington Avenue
P. O. Box 1069
Madison, WI 53701-1069
(608) 256-8356
Attorney for Defendant-Appellant,
Jacob R. Beyer

CERTIFICATION OF BRIEF

I hereby certify that this brief conforms to the rules contained in § 809.19(8)(b) and (c) for a brief produced with a proportional serif font. The length of this brief is 10,909 words.

I further certify that the text of the electronic copy of this brief is identical to the text of the paper copy of the brief.

Dated this 13 day of March, 2023.

EISENBERG LAW OFFICES, S.C.

Mark A. Eisenberg
State Bar Number: 1013078
308 E. Washington Avenue
P. O. Box 1069
Madison, WI 53701-1069
(608) 256-8356

Attorney for Defendant-Appellant,
Jacob R. Beyer

CERTIFICATION OF COMPLIANCE WITH
§ 809.19(12), WIS. STATS.

I hereby certify that I have submitted an electronic copy of this brief, excluding the appendix, if any, which complies with the requirements of § 809.19(12), Wis. Stats.

I further certify that the electronic brief is identical in content and format to the printed form of the brief filed as of this date.

A copy of this certificate has been served with the paper copies of this brief filed with the Court and served on all opposing parties.

Dated this 13 day of March, 2023.

EISENBERG LAW OFFICES, S.C.

Mark A. Eisenberg
State Bar Number: 1013078
308 E. Washington Avenue
P. O. Box 1069
Madison, WI 53701-1069
(608) 256-8356

Attorney for Defendant-Appellant,
Jacob R. Beyer

## CERTIFICATION OF APPENDIX

I hereby certify that filed with this brief, either as a separate document or as a part of this brief, is an appendix that complies with § 809.19(2)(a) and that contains: (1) a table of contents; (2) the findings or opinion of the circuit court; and (3) portions of the record essential to an understanding of the issues raised, including oral or written rulings or decisions showing the circuit court's reasoning regarding those issues.

I further certify that if this appeal is taken from a circuit court order or judgment entered in a judicial review of an administrative decision, the appendix contains the findings of fact and conclusions of law, if any, and final decision of the administrative agency.

I further certify that if the record is required by law to be confidential, the portions of the record included in the appendix are reproduced using first names and last initials instead of full names of persons, specifically including juveniles and parents of juveniles, with a notation that the portions of the record have been so reproduced to preserve confidentiality and with appropriate references to the record.

I further certify that content of the electronic copy of the appendix is identical to the content of the paper copy of the appendix.

Dated this 13 day of March, 2023.

EISENBERG LAW OFFICES, S.C.

Mark A. Eisenberg
State Bar Number: 1013078
308 E. Washington Avenue
P. O. Box 1069
Madison, WI 53701-1069
(608) 256-8356
Attorneys for Defendant-Appellant,
Jacob R. Beyer