STATE OF WISCONSIN

SUPREME COURT

STATE OF WISCONSIN,

Plaintiff-Respondent,

vs. Appeal No. 2022AP2051-CR

JACOB R. BEYER,

Defendant-Appellant.

PETITION FOR REVIEW AND APPENDIX OF DEFENDANT-APPELLANT

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

TABLE OF AUTHORITIES

Cases **Page**

Statutes

Other Materials

ISSUE PRESENTED FOR REVIEW

1. Did the trial court and the Court of Appeals err in denying Beyer's request for an order permitting forensic analysis of the State's investigative computer system in order to challenge its reliability after that computer allegedly detected a single file containing child pornography which constituted the primary basis for law enforcement's application for a search warrant of Beyer's home and electronic devices, even though said file was never recovered or produced following execution of the search warrant?

Beyer submits that this denial violated his due process rights under the 5th, 6th , and 14th amendments to the United States Constitution in that it deprived him of a meaningful opportunity to pursue a motion to suppress and thereby to mount and present a complete defense . Beyer further submits that, in the context of a situation where a warrant affidavit alleges a computerized detection of a singular item of evidence justifying the issuance of search warrant and said evidence subsequently proves to be unfound or undetected in the course of executing the warrant, the right to mount a complete defense and therein challenge the reliability of the inceptive computerized detection supersedes the dictates of Wis. Stat. §971.23 and should allow

for a defense analysis of the computer system at issue. Beyer urges this Court to find that denying him the ability to forensically analyze the State's computer system on the grounds that the State did not intend to offer evidence relating to the missing file at trial effectively rendered the meaningful pursuit of a motion to suppress an impossibility as it allowed him no means of interrogating the reliability or credibility of the source from which the inceptive inculpatory information and allegations originated, which should be deemed tantamount to a deprivation of due process. Beyer would assert that, in any adjacent investigatory context, the wholesale foreclosure of any opportunity to challenge the credibility or reliability of the solitary source of inculpatory information underlying a search warrant as a matter of course would be deemed constitutionally impermissible.

In the trial court, Beyer asked for an opportunity to forensically analyze the State's computer utilizing undercover investigative computer software ("UIS") which allegedly established a peer-to-peer ("P2P") connection with a device at Beyer's registered internet protocol ("IP") address and 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 the search warrant at Beyer's residence, and despite the parties' apparent agreement both that the software involved was vulnerable to malware and that the alleged file's existence or absence at the relevant place and time

could likely be ascertained via forensic analysis of the investigative computer, the trial court denied Beyer's discovery request for forensic analysis of the computer pursuant to Wis. Stat. §971.23. Despite Beyer's invocation of his constitutional right to that discovery pursuant to the guarantees of due process, the trial court found that Beyer was not entitled to the discovery as the State did not intend to offer evidence of the missing image at trial.

The Court of Appeals affirmed the trial court's decision, dismissing Beyer's "novel argument" that due process warranted the forensic analysis of the State's computer system while reiterating the notion that the fact that his request did not directly implicate "trial evidence" reduced the constitutional concern for scrutiny or redress. Regardless, and despite acknowledging that Beyer's expert witness testified that the UIS was subject to malware which could be used to manipulate files on Beyer's computer, the Court found that Beyer had failed to establish the necessary materiality or a reasonable probability of a different outcome which would warrant a reversal of the trial court decision on constitutionality grounds (A: 15-16).

STATEMENT OF THE CRITERIA IN § 809.62(1) WHICH SUPPORT GRANTING THE PETITION

This Court should accept review of this case for the following reasons:

1. A real and significant question of constitutional law is presented concerning a defendant's right to pretrial discovery in the context of prosecutions underpinned by the use of undercover investigative software, which is a relatively novel and rapidly evolving area of law enforcement investigations.

2. A decision by the Supreme Court will help clarify and reconcile this State's discovery statutes with a defendant's due process rights under federal law in a novel area of concern which will have statewide impact as conflict over what discovery a defendant is entitled to in child pornography prosecutions, largely due to the inscrutability of the underlying law enforcement tools of investigation, repeatedly arises in such cases.

3. The Court of Appeals' reasoning in its decision on the issue presented is circular and unworkable in light of due process jurisprudence—a defendant in Beyer's position cannot ever demonstrate "a potential violation of his rights" by a specific law enforcement apparatus if he or she is categorically deprived of any means of meaningfully interrogating the

reliability or credibility of that apparatus. The State, by deft exploitation of the "intends to offer...at trial" provision of Wis. Stat. § 971.23(1)(g), avoids any scrutiny of its frequent inability to recover the specific evidence allegedly detected by its undercover investigative software by simply electing to only issue charges for other materials that are found upon execution of warrants based on those unconfirmed alleged detections. By allowing this system of proceeding to persist, courts are essentially endorsing the idea that the "ends justify the means" in these cases, which is antithetical to the notion of due process and the exclusionary rule.

STATEMENT OF THE CASE

The Court of Appeals recitation of the facts is not detailed and therefore Beyer feels compelled to supplement it to some extent here. 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, (R.55:15).

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 individual "who ha[s] an interest in child pornography or child sexual exploitation." 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]

---

[1] At trial on August 30, 2022 the State's forensic expert testified that she could not determine if Beyer ever knew the illicit file was on his device (R. 175:46), and Lenzer testified to the same at the suppression hearing (R.66:27-8)

The Search warrant was executed on 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). 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. (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). However, the trial court invited Beyer to file a suppression motion to offer testimony through his own experts in support of a challenge to the warrant's validity. (R.95:24-25).

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 Beyer 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. 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). 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 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

---

[2] At trial on August 30, 2022, Lenzner again 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).

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 obtain the search warrant was only charged once or twice. (R.66:62-64).[3] 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).

[3]Presumably so the State would not have to provide the defense with an opportunity to examine the computer pursuant to Wis. Stats. §971.23(5).

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). 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).

In rendering a decision, the trial court stated 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." (R.66:66). 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). 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).

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).

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 Beyer was the party who would be in possession of it, as "[t]he mere presence in [the agent's] file on his computer I think is sufficient...for that purpose." (R.66:79-83). 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," thereby denying Beyer's motion in "a very, very close call." (R.66:82-83). A final order for the purpose of appeal was signed by the trial court on April 1, 2019. (R.65; A:44).

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:45-46).

Beyer subsequently proceeded to a court trial on August 30, 2022. (R.175). The State ultimately agreed to proceed to trial to the court on Count 1 of the original complaint only. (R.146-147, 149). Beyer was convicted and sentenced to four years in the Wisconsin State Prison System which consisted of three years of initial confinement and one year of extended supervision (R.85; A:47-48). That sentence was stayed pending Beyer's appeal of several issues, only one of which he is seeking review of here.

In its decision on the issue presented for review in this petition, the Court of Appeals concluded that Beyer had neither shown a violation of his rights nor established a "reasonable probability of a different outcome for his motion to suppress" if he had been given access to the state's computer in order to test its reliability. (A:15-16). Notwithstanding the fact that the state agent and the defense expert agreed that the relevant computer program was subject to malware or that the defense expert testified that he could likely determine whether that vulnerability had been exploited on Beyer's computer by analyzing the State's

computer, the Court found that Beyer's arguments were "heavily speculative" and otherwise "amount[ed] to potential policy concerns" not demonstrating reversible error. (A:16).

ARGUMENT

I. THE DEPRIVATION OF AN OPPORTUNITY TO FORENSICALLY EXAMINE THE STATE'S COMPUTER AND UIS VIOLATED BEYER'S SUPERSEDING DUE PROCESS RIGHTS.

Both the trial court and the appellate court concluded that Wis. Stat. § 971.23 did not provide grounds for Beyer's discovery request because the State represented that the evidence retrieved by the UIS would not be used at trial. Beyer would maintain that his due process rights mandate the disclosure in the context presented here, where a search warrant was issued because of an alleged computerized detection of a single file of illegal material that was never produced or recovered in the course of executing that warrant, and where the defendant has offered an articulable theory as to how the inceptive detection may have been erroneous or otherwise due to conduct not attributable to the defendant.

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. Moreover, he would note that 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.[4]

---

[4] The Court of Appeals admitted that there is federal case law supporting his argument that failure to disclose information or evidence that is material to a "potential" fourth amendment violation can violate his constitutional right, but concluded that the federal cases are based upon Rule 16 of the Federal Rules of Criminal Procedure which was broader than applicable constitutional or Wisconsin statutory discovery right(A:12).

However, for guidance—Beyer would look to case law which outlining the 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). 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. At the very least, he submits that he articulated a non-speculative theory as to how the missing file may have ended up on his computer through no fault of his own to the most developed extent that any defendant could without ever being permitted to analyze the system which allegedly reported the detection. In other words, Beyer submits, if the bar to establish materiality is above what Beyer's experts articulated here, any attempt to establish materiality in this specific context by any defendant facing a similar situation is predestined to fail before a word is uttered because the State can always utilize

Wis. Stat. § 971.23 as a shield to prevent a defendant from accessing the only source of information that could possibly tip the materiality scale in his or her favor. This prohibitive state of play, he submits, is fundamentally unfair and incompatible with any reasonable understanding of what process due process actually entails.

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 admittedly 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.[5] 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

[5]The Court of Appeals concluded that though the state agent testified that the UIS was subject to malware, he also indicated had never experienced a malware infection and therefore there was nothing from which the Court could conclude that there was a reasonable probability that a different outcome would occur if the discovery request was granted (A-15-16).

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.[6]

---

[6] The reasoning in *Budziak* was used by the District Court in *United States v. Crowe,* 2013WL12335320,(D.N.M. Apr. 3, 2013), to grant the defendant's motion to allow his forensic expert to

Similarly, 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

---

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. Beyer would also note that the Court there dispensed with the Government's arguments akin to the State's "use at trial" arguments offered in this case:

> Furthermore, the Court does not agree with the government's argument that the evidence sought is "ancillary" as discussed in *United States v. Price*, 75 F.3d 1440 (10th Cir. 1996). The evidence sought in this case is quite critical to the government's case-in-chief against Defendant. Defendant is not obligated to merely defer to the government's word that his own separate investigation would be unfruitful.

Crowe at *7.

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.*

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.

Although reaching a different result due to the specific circumstances presented in the case, the Court in *United States v. Pirosko*, 787 F.3d 358 (6th Cir. 2015) echoed the rationale of the courts in *Budziak* and *Gonzales*. In *Pirosko*, the defendant requested that the government disclose the law enforcement tools and records used to search the defendant's computer equipment, claiming the search warrant was obtained using unreliable and unsupported information. There, the officer had connected to the defendant's file sharing network numerous times while the defendant moved about the country. In support of his motion the defendant again cited *Budziak*. Despite that

invocation, the Court held that Pirosko had failed to cast any doubt on the government's testimony that it had provided verified files of what had been downloaded by the government agent—something which never occurred in Beyer's case. Furthermore, in deciding the case the court specifically admonished that

> this conclusion should not be read as giving the government a blank check to operate its file-sharing detection software sans scrutiny. As a general matter, it is important that the government's investigative methods be reliable, both for individual defendants like Pirosko and for the public at large. Still, we think that it is important for the defendant to produce some evidence of government wrongdoing.

Id. at 366. The Court went on to explain that

> Pirosko has failed to produce any such evidence here, even after receiving the government's computer logs, which included information on when law enforcement officials were able to connect to his computer and what files they were able to download from his shared folder.

By contrast, the Court referred to the aforementioned *United States v. Crowe*, 2013WL12335320 (D.N.M. Apr. 3, 2013), as an exemplar for the defendant meeting his or her burden in moving for an independent evaluation of similar government software, stating

> in reaching this decision, the district court noted that, "[a]s in *Budziak*, in this case, Defendant submitted the testimony of his expert witness, Tami Loehrs, who indicated that during her examination of Defendant's computer, some of the files alleged to have been found by law enforcement in the shared space of Defendant's computer, were not found there during her analysis." Pirosko has, as we have already noted, not submitted any such evidence.

Id. at 367.

In Beyer's case, the defense expert testimony coupled with the fact of the missing file should have been enough for the court to grant his motion along the same lines of reasoning. 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 any time much less the time of the alleged download. Apparently, since that is something that law enforcement is 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 made the requisite showing of materiality under the relevant precedential framework. The due process clause

requires the specific discovery he requested in this type of case; Beyer submits that his constitutional rights should not be relegated to the backseat by Wis. Stat. § 971.23. See *Arizona v. U.S.* 567 U.S 387, 132 S.Ct. 2492(2012).

Depriving Beyer and other defendants from this type of discovery gives the State unfettered authority to use the UIS to make a bare-bones allegation in order to obtain search warrants and then avoid any scrutiny as to the processes underlying that allegation even when the material specifically identified in that allegation proves to be non-existent. This issue comes up frequently in child pornography cases.[7] In other conceptually-adjacent cases, the defendant is allowed to contest the reliability of the information used to obtain a search warrant. For example, when the State uses drug dogs to support a request for a search warrant, the defendants in those cases are allowed to review and challenge the reliability of the dogs by reviewing the dog's records, presumably even if the State elects not to charge the specific contraband upon which the dog alerts. *See State v. Miller,* 256 Wis.2d 80, 89, 2002 WI APP ¶12 (a drug-sniffing dog provides sufficient evidence for a search so long as the dog is trained and has demonstrated a sufficient level of reliability in the past). Beyer is asking to be afforded a similar opportunity in

[7]This attorney has defended many cases involving child pornography and file-sharing networks which were used to transmit child pornography.

this context—where he has raised specific questions about the reliability of the system in question through both the fact of missing evidence and expert testimony—which he submits that due process demands.

CONCLUSION

For all of the foregoing reasons, Beyer respectfully asks this Court to accept this Petition for Review and establish a briefing schedule on the issues.

Dated this 8th day of February, 2024.

EISENBERG LAW OFFICES, S.C.

Electronically Signed By:
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 petition conforms to the rules contained in § 809.19(8)(b) and (bm) and § 809.62(4) for a brief produced with a proportional serif font. The length of this brief is 7,952 words.

Dated this 8th day of February, 2024.

EISENBERG LAW OFFICES, S.C.

Electronically Signed By:
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.

Dated this 8th day of February, 2024.

EISENBERG LAW OFFICES, S.C.

Electronically Signed By:

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.

Dated this 8th day of February, 2024.

EISENBERG LAW OFFICES, S.C.
Electronically Signed By:
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