No. 125550

IN THE
SUPREME COURT OF THE STATE OF ILLINOIS

THE PEOPLE OF THE STATE OF ILLINOIS Plaintiff-Appellant	)	Appeal from the Appellate Court of Illinois, Third District, No. 3-17-0830
vs.	)	There on appeal from the Circuit Court of the Tenth Judicial Circuit, Peoria County, Illinois No. 14 CF 282
JOHN T. McCAVITT Defendant-Appellee	)	Honorable David Brown & Albert Purham Judges Presiding

RESPONSE BRIEF OF DEFENDANT-APPELLEE

JOSHUA B. KUTNICK
900 West Jackson Blvd., Ste. 7E
60607, 312-441-0211
joshua@kutnicklaw.com

JAMES K. LEVEN
203 North LaSalle Street, Ste. 2100 Chicago, IL
Chicago, IL 60601, 312-558-1638
jameskleven@attorneyleven.com

Counsels for Defendant-Appellee, John McCavitt

ORAL ARGUMENT REQUESTED

E-FILED
3/3/2021 10:34 PM
Carolyn Taft Grosboll
SUPREME COURT CLERK

TABLE OF CONTENTS

POINTS AND AUTHORITIES

STATEMENT OF FACTS

Defendant-Appellee adopts the facts as presented by the appellate court. *People v. McCavitt,* 2019 IL App (3d) 170830. Defendant-Appellee will also discuss specific facts in the relevant argument portions of this brief.

ARGUMENT

Summary statement

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const., amend. IV.

John McCavitt's constitutional claim consists of three basic elements. First, McCavitt will show that the police executed a search of the exact duplicate of his computer hard drive within the meaning of the Fourth Amendment under both the U.S. Supreme Court's property and privacy-based approaches. Second, the search was unreasonable and violated the Fourth Amendment because the police did not obtain a warrant supported by probable cause before embarking on the search. Third, the evidence from the unconstitutional search should be suppressed. Consequently, without the suppressed evidence, the State has insufficient evidence to support a conviction, and the conviction should be reversed outright. This Court should affirm the Appellate Court's order reversing the trial court's denial of McCavitt's motion to suppress. *See People v. McCavitt,* 2019 IL App (3d) 170830.

Standard of Review

In reviewing a trial court's ruling on a motion to suppress evidence, this Court employs the two-part standard of review adopted by the U.S. Supreme Court in *Ornelas v. United States*, 517 U.S. 690 (1996). *See People v. Hill*, 2020 IL 124595, ¶ 14. Under this standard, a court may reverse the trial court's findings of fact if they are against the manifest weight of the evidence. *Id*. However, a court may evaluate the established facts in relation to the issues and may draw its own conclusions in deciding what relief, if any, should be granted. *Id*. A court reviews *de novo* the ultimate conclusion whether suppression of evidence is warranted. *Id*.

I. Detective Feehan conducted a search on the exact duplicate of McCavitt's original hard drive.

A. Whether Detective Feehan conducted a search and whether that search was reasonable are separate and distinct constitutional questions whose analysis should not be commingled.

A proper Fourth Amendment analysis focuses on two related but separate questions: The first issue is whether the police have conducted a search within the meaning of the Fourth Amendment. The second issue assumes that a search occurred and asks whether it was constitutionally reasonable. *See United States. v. Correa*, 908 F.3d 208, 217 (7th Cir. 2018) ("The Fourth Amendment essentially asks two questions: first, has there been a search or a seizure, and second, was it reasonable?"); *Carpenter v. United States*, 138 S. Ct. 2206, n.2 (2018) (suggesting that courts should avoid "conflat[ing] the threshold question whether a 'search' has occurred with the separate matter of whether the search was reasonable."); *Arizona v. Hicks*, 480 U.S. 321, 324, 325 (1987) (examining first whether the officer's actions constituted a search or seizure and then whether those actions were reasonable under the Fourth Amendment.) McCavitt will show in Issue I that Feehan conducted a Fourth Amendment search and, in Issue II, that the search was unreasonable because he did not first obtain a warrant before starting the search.

B. This Court should apply *both* a property and privacy-based approach to determine whether the police conducted a Fourth Amendment search.

To determine whether a search has occurred in any given case, this Court has recently held that it considers both property and privacy-based approaches to determine the meaning and proper application of the Fourth Amendment. *See People v. Lindsey*, 2020 IL 124289, ¶¶ 16-18. Conspicuously absent from the State's opening brief is any discussion of *Lindsey*. The State also does not consider whether this Court is required to consider and apply both approaches. The State's analysis is entirely confined to a privacy-based approach, contrary to the recent teachings of *Lindsey*.

McCavitt asks this Court to apply both frameworks as this Court did in *Lindsey*. *See Lindsey*, 2020 IL 124289 at ¶ 18. ("If, as the State contends, the warrantless dog sniff here did not violate the fourth amendment under the privacy-based approach, we still must determine whether it violated the fourth amendment under the property-based approach. Thus, we will address both approaches in turn.") *Lindsey's* reading of U.S. Supreme Court precedent not only permits but encourages the parties to present a two-pronged analysis of the constitutionality of a search or seizure, one premised on historical notions of private property, the other on a modern conception of society's understandings of privacy. *See Id.*

The *Lindsey* Court criticized the State and the defense for failing to brief a property-based Fourth Amendment claim. *Id.* ("The parties focus almost solely on the privacy-based approach.") Despite the lack of briefing on the subject, the *Lindsey* Court moved forward with analyzing Fourth Amendment claims based on private property (as well as a privacy-based approach) even though the defendant in *Lindsey* did not present such a property claim. *Id*. (rejecting defendant's contention that a property-based approach to the Fourth Amendment was not necessary to

resolve the defendant's claim and addressing the merits despite the defendant's erroneous understanding).

In terms of sequencing of claims, McCavitt asks this Court to examine the property-based approach first and then to follow with his privacy arguments. *See People v. Bonilla*, 2017 IL App (3d) 160457, ¶ ¶ 12-13 ("If applicable, the property-based approach should be applied first."); *aff'd on other grounds*, 2018 IL 122484; *United States v. Sweeney*, 821 F.3d 893, 899 (7th Cir. 2016) ("We address first the approach focused on the common law of property and whether the police committed a trespass when conducting the search.")

C. The property-based approach

1. The property-based approach applied to the Fourth Amendment

The police conducted a Fourth Amendment search of McCavitt's mirrored hard drive under the property-based approach. To analyze his claim under that rubric, this Court should identify and apply the correct mode of analysis. The U.S. Supreme Court has formulated the following basic test for determining whether the government has initiated a Fourth Amendment search: "When the Government obtains information by physically intruding on persons, houses, papers, or effects, a search within the original meaning of the Fourth Amendment has undoubtedly occurred." *Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) (internal quotations omitted). Expounding on this concept, the Court in *Jardines* found that the Fourth Amendment text "indicates with some precision the places and things encompassed by its protections: persons, houses, papers, and effects." *Jardines*, 133 S. Ct. at 1414 (internal quotation omitted). This Court in *Lindsey* explained that *Jardines* "exemplif[ies]" "the property-based approach." *Lindsey*, 2020 IL 124289, ¶ 17.

Framed similarly to *Jardines*, the Court determined in *United States v. Jones*, 132 S. Ct. 945, 949 (2012) that a police officer conducts a search when he or she "physically occupie[s]

private property for the purpose of obtaining information." For most of our constitutional history the Fourth Amendment was understood to mean that the police infringe on interests protected by the Fourth Amendment, and therefore conduct a search, if they trespass upon areas enumerated by the Fourth Amendment: "persons, houses, papers, and effects." *Jones*, 132 S. Ct. at 950. The above-cited standards from *Jardines* and *Jones* are based on the text of the Fourth Amendment, the original historical understandings of the purposes of the Amendment, and the property interests it was intended to protect.

The property-based standard embraced in *Jardines* and *Jones* provided the exclusive means for Fourth Amendment protection for most of American history. *See Jardines*, 133 S. Ct. at 1414; *Lindsey*, ¶ 20; *Jones*, 132 S. Ct. at 949 ("The text of the Fourth Amendment reflects its close connection to property.") "Lower courts recognized *Jones* (and *Jardines*) as a sea change," *United States. v. Richmond*, 915 F.3d 352, 357 (5th Cir. 2019). This line of authority revived a property-based approach that the *Katz* reasonable expectancy of privacy formula appeared to jettison. *See United States v. Sweeney*, 821 F.3d 893, 899 (7th Cir. 2016) citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan J. concurring).

Examining the facts of *Jardines* and *Jones*, the Court determined that the police had executed a search in both cases. In *Jardines*, police officers accompanied by trained dogs physically entered and occupied the curtilage of the defendant's home to conduct a criminal investigation and obtain information. *Jardines*, 133 S. Ct. at 1414. The Court determined that such an intrusion into a constitutionally protected area was a search under the original meaning of the Fourth Amendment. *See id.* at 1418. Similarly, in *Jones*, the police placed a GPS tracking device on the defendant's car to acquire information on the vehicle's whereabouts. *Jones*, 132 S. Ct. at 949. The Court held that the GPS tracking investigation was a search because the police

occupied private property, a constitutionally protected area, for the purpose of obtaining information. *Id.*

Using the property-based construct to determine whether a search has occurred is "easy." *See Jardines*, 133 S. Ct. at 1417 ("One virtue of the Fourth Amendment's property-rights baseline is that it keeps easy cases easy.") Even minimal, insignificant intrusions constitute a search under the common law property-based approach. *See United States v. Richmond*, 915 F.3d 352, 357-59 (5th Cir. 2019) (Tapping of a tire on a vehicle stopped by a police officer was a search under *Jones* "regardless of how insignificant it might seem."); *Id*. (Tapping of a tire is a common law trespass and therefore a search when "conjoined with an attempt to find something or obtain information.") (internal quotation marks omitted). The U.S. Supreme Court's property-based trespass analysis on Fourth Amendment questions is "simplistic," more predictable, and less problematic than determining whether a person has a reasonable expectation of privacy through examining and applying contemporary norms of conduct. *See Richmond*, 915 F.3d at 359.

2. Property-based approach applied to this case

Applying the property-based approach as discussed in *Jones* and *Jardines* to the present case shows that the police conducted a Fourth Amendment search of an exact duplicate of McCavitt's hard drive. (R17.) On July 17, 2013, McCavitt owned and possessed his desktop tower, personal computer and accompanying hard drive when the police seized it from his home as a result of the July 2013 warrants. (R10.) McCavitt did not use the computer in any way for his job as a police officer with the Peoria Police Department. (R11.) The Peoria Police Department did not have any possessory interest or claim to the computer. (R11.) After McCavitt's acquittal on all charges in Case No. 13-CF-741 on March 19, 2014, McCavitt, through his counsel, asked the court to direct the police to return all items seized from him

pursuant to the warrants, which included his computer and hard drive, and the personal digital information contained therein. (R11-12.) These items have never been returned to McCavitt. (R11-12.)

Because McCavitt's computer and its accompanying hard drive that the police seized were his private property, as that concept was understood at the founding of our Constitution, they should be considered "effects" within the scope and meaning of the text of the Fourth Amendment. *See, e.g.*, *People v. Gingrich*, 862 N.W.2d 432, 436 (Mich. Ct. App. 2014) ("It can hardly be doubted that a computer, which can contain vast amounts of personal information in the form of digital data, is an 'effect[],' … within the meaning of the constitutional proscription against unreasonable searches and seizures"); *United States v. Christie*, 717 F.3d 1156, 1164 (10th Cir. 2013) ("Personal computers … can contain (or at least permit access to) our diaries, calendars, files, and correspondence — the very essence of the 'papers and effects' the Fourth Amendment was designed to protect."); *Compare Wisconsin v. Tate*, 849 N.W.2d 798 at 822, ¶ 96 (Wisc. Sup. Ct. 2014) ("The defendant's cell phone is private personal property, a constitutionally protected personal 'effect.'") *with Riley v. California*, 134 S. Ct. 2473, 2489 (2014) (identifying the cell phone as a mini-computer).

After having seized McCavitt's personal property, including his personal computer and hard drive, the police examined his digital information to find evidence of criminal activity. Detective Jeffrey Avery of the Peoria County Sheriff's Department testified that he received McCavitt's personal property that was seized from his residence pursuant to the July 2013 warrants. (R14-16.) Avery, a forensic examiner, examined McCavitt's computer, removed the hard drive and made an exact copy, or mirror image, of the contents of the hard drive using EnCase software. (R17.) A copy of the hard drive, called "EnCase evidence file," was saved on

Avery's computer. (R17); *McCavitt*, 2019 IL App (3d) 170830 ¶ 4. Avery performed a search for video and images but no child pornography was discovered. (R422-424.) On March 21, 2014, a few days after McCavitt's March 19, 2014 acquittal on Case No. 13-CF-741, Avery received a call from Detective James Feehan of the Peoria Police Department, asking if he could copy and send him the evidence on an external hard drive. (R17-18.) Avery made another copy of the EnCase evidence file and sent it to Feehan. (R19, 26.)

Detective James Feehan testified that, relative to the case on which the July 2013 search warrants were issued, McCavitt was acquitted on the charges from that case on March 19, 2014. (R29.) Feehan testified that on March 20, 2014, the day after the acquittal, the Peoria Police Department launched an internal investigation of McCavitt, a police officer with the department. (R30.) The internal investigation was running parallel to a criminal investigation. (R40.) On March 21, 2014, Feehan, also a forensic examiner, requested and received the copy of the EnCase file from Avery. (R30.) Feehan testified that he knew "that there was [sic] other victims that could be identified during the formal that would turn criminal." (R32-34.) On March 24, 2014, Feehan conducted a digital analysis on the EnCase file copy and saw two images he believed to be child pornography. (R33); *McCavitt*, 2019 IL App (3d) 170830 ¶ 5.

The mirrored digital files, information, and images Feehan examined from McCavitt's duplicated hard drive are unmistakably constitutionally protected property and thus "papers" within the scope of this term's original meaning. *See, e.g.*, *People v. Thompson*, 51 Misc. 3d 693, 727 (Sup Ct. 2016) ("Computer records for most of us are the modern day equivalent of the 'papers' whose indiscriminate search the founders so deeply abhorred."); *United States v. Ganias*, 755 F.3d 125, 135 (2d Cir. 2014) ("Like 18th Century 'papers,' computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should

be similarly guarded against unwarranted Government intrusion. If anything, even greater protection is warranted."); *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (noting that the Framers were prescient about guaranteeing the sanctity of "papers" from unreasonable search because "[t]he papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities."); *Id.* at 964 (digital documents "implicate[] the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers'"). As the *Cotterman* Court found:

> The Framers listing of papers within the scope of the Amendment "reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas — what we might call freedom of conscience — from invasion by the government.

Cotterman, 709 F.3d at 964.

Following closely on the heels of McCavitt's acquittal, Feehan's thorough, detailed, meticulous, and extensive examination of the mirrored hard drive that was created from McCavitt's private property (e.g.: his computer, hard drive, digital files, and digital information), in order to gather evidence in an investigation, constituted a Fourth Amendment search. *See Tate*, 849 N.W.2d at 822, ¶ 96 ("A physical intrusion into … property with intent to find information creates a trespassory search."); *id.* at n. 54 ("Courts have treated government intrusions into stored data on computers as trespasses to a chattel.").

3. McCavitt's substantial property right to his personal information stored on his hard drive, including the right to exclude others, extends to the hard drive exact duplicate that the police created from his original.

(Response to State's Brief at Part B.)

Without addressing the U.S. Supreme Court's property-based framework for analyzing the Fourth Amendment or even acknowledging *Jardines* and *Jones* as binding precedent, the State argues that the police did not perform a search because McCavitt did not own or have a

possessory interest in the hard drive copy that the police duplicated from his original. (St. Br. at 17, 20.) The State's argument should be rejected. Feehan's examination of the police-generated forensic copy of McCavitt's original for information pertaining to a criminal investigation is no less a search and no less an infringement on his property rights than had Feehan examined the original. As shall be discussed more extensively below, Feehan's post-acquittal examination of the information contained in the duplicate hard drive infringed on McCavitt's fundamental property right to exclude others, including and especially the police, from accessing, using and gaining information from McCavitt's private property. Contrary to the State's claim, the police performed a search.

As the U.S. Supreme Court explained in the Fourth Amendment context, "One of the main rights attaching to property is the right to exclude others[.]" *Byrd v. United States*, 138 S. Ct. 1518, 1527 (2018) quoting *Rakas v. Illinois*, 439 U.S. 128 n. 12 (1978) citing W. Blackstone, Commentaries, Book 2, ch. 1. Emphasizing the vital importance attached to the right to exclude, the Court has held that the "right to exclude" is "universally held to be a fundamental element of the property right." *Kaiser Aetna v. United States*, 444 U.S. 164, 179-180 (1979); *Loretto v. Teleprompter Manhattan CATV Corp*. 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights."); *see also International News Service v. Associated Press*, 248 U.S. 215, 250 (1918) (Brandeis, J., dissenting) ("[a]n essential element of individual property is the legal right to exclude others from enjoying it.") Authoritative commentators have also explained the bedrock, fundamental nature of the right. *See, e.g.*, Thomas W. Merrill, *Property and the Right to Exclude*, 77 Neb. L. Rev. 730, 730, (1998) ("Deny someone the exclusion right and they do not have property."); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths*

and the Case for Caution, 102 Mich. L. Rev. 801, 813 (March 2004) ("The right to exclude others [is] the very essence of the property right.").

As the revered authority on the English common law, William Blackstone, stated on the exclusive nature of property ownership: "There is nothing which so generally strikes the imagination, and engages the affections of mankind, as the right of property; or that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe." 2 W. Blackstone, Commentaries on the Laws of England *2.

The police-generated creation of a mirrored hard drive from McCavitt's original enabled Feehan to examine the functional equivalent of the original in his quest to connect McCavitt to criminal activity. The mirrored hard drive is exactly the same as the original with all digital files and images identical to the originals. Feehan's commandeering of McCavitt's personal, digital information was a significant encroachment on McCavitt's exclusive right to keep others from accessing, using, and benefitting from his personal, private property. Since the property right to exclude as understood at the time of the framing belonged to McCavitt, and certainly not the police, Feehan trammeled on McCavitt's exclusive right when he examined the exact duplicate of McCavitt's original hard drive for evidence of criminal activity.

In a similar context, a court held that the taking of high-resolution photographs and making copies of documents is both a search and seizure within the meaning of the Fourth Amendment. *United States v. Jefferson*, 571 F. Supp. 2d 696, 704 (E.D. Va. 2008). The court found that copying interferes with the owner's sole possession and interest in privacy of the information contained in the documents. *Id.* at 703. Reinforcing this concept, the court in *United*

States v. Loera, 333 F.Supp.3d 172, 185-86 (E.D. N.Y. 2018) found that digital duplication interferes with the owner's control over the information contained in the digital medium.

The overriding principle to be gleaned from *Jefferson* and *Loera* is that copying of digital information deprives the owner of his sole right to bar other persons or entities such as the government from gaining access to the information and knowledge that can be acquired from viewing the digital data. Such copying and examining impermissibly interferes with the owner's exclusive right to control over that information from infringement by others. *See Byrd*, 138 S. Ct. at 1527 (right to exclude others is the paramount component of the common law property right that forms the basis for the Fourth Amendment); *see also Loretto*, 458 U.S. at 435 (similar).

In order to demonstrate a search under a property-based theory, the defendant needs to establish a trespass conjoined with an attempt to find something or obtain information. *Jones*, 132 S. Ct. at 951 n. 5. In *Jones*, the Court found that a search was conducted because police placed a GPS monitor on a suspect's car to acquire information on the suspect's movements. In the present case, similar to *Jones*, the police infringed on McCavitt's exclusive right to control his property by seizing his computer and making a forensic copy of his original hard drive containing his own personal information stored on his computer without his permission. The police, here, consummated a search by examining McCavitt's personal information on the exact duplicate of the hard drive for the purpose of conducting a far-ranging exploration for evidence of criminal activity. It makes no constitutional difference that the examination was conducted on an exact forensic duplicate instead of the original; a search was consummated regardless because the police actively encroached upon and investigated McCavitt's private digital information to conduct a criminal probe.

4. Because McCavitt has established a search under the property-based model, he is not required to show his reasonable expectation of privacy was violated to establish a search.

(Response to State's Brief at Part A.1.)

The State maintains that Detective Feehan did not conduct a Fourth Amendment search because his "second look" post-acquittal examination of the mirrored hard drive occurred when McCavitt had a non-existent or reduced expectation of privacy in his property. (St. Br. at 11-15.) The State's arguments are misplaced because, as shall be shown below, McCavitt had substantial privacy interests that were invaded by Feehan's conduct. (*See* Part I.G. *infra.*) Regardless, McCavitt's privacy interests are not determinative. He is not required to prove that he had an expectation of privacy in his computer, his hard drive, the forensic duplicate of the hard drive, or his personal information stored on these electronic devices in order to show that the police performed a search.

Defendants need not establish that privacy rights were invaded to show that a search occurred under the property-based framework. *See People v. Martin*, 2017 IL App (1st) 143255, ¶ 32 (declining to consider whether the defendant's reasonable expectation of privacy under *Katz* was violated, because the police conducted a search under *Jardines* by gaining evidence by physically intruding on a constitutionally protected area); *Taylor v. Rodriguez*, Case No. 16-cv-8159, 2018 WL 4635647, at *5 (N.D. Ill. 2018) ("[W]hether Plaintiffs had a reasonable expectation of privacy is not dispositive of Plaintiffs' Fourth Amendment search claim" because of the U.S. Supreme Court's property-based approach to Fourth Amendment analysis). The U.S. Supreme Court has found that the *Katz* reasonable expectation of privacy test did not extinguish and replace the Court's historical property-based approach. *See Byrd*, 138 S. Ct. at 1526 (holding that the legitimate expectation of privacy test "supplements rather than displaces" the historical property-based approach); *Jardines*, 133 S. Ct. at 1417 ("[T]he *Katz* reasonable-expectation-of-

privacy test has been *added to*, not *substituted for*, the traditional property-based understanding of the Fourth Amendment.") (emphasis in the original); *People v. Burns*, 2016 IL 118973, ¶ 23 (*Katz* adds to the constitutional baseline of Fourth Amendment protections but does not eliminate the Amendment's property rights protections).

This Court should find that the police executed a Fourth Amendment search, regardless of whether they violated McCavitt's reasonable expectation of privacy. The State's claim that McCavitt had reduced expectations of privacy fails because it does not account for the property-based approach that this Court faulted the State and the defense for failing to raise and apply in *Lindsey*. *See* Part I.B. *supra*. It makes no constitutional difference whether McCavitt expected the information stored on his hard drive to remain private when Feehan conducted his examination of the digital information contained in the forensic duplicate of McCavitt's hard drive. What matters is that McCavitt's property rights were violated.

D. The privacy-based approach

1. Detective Feehan conducted a search because he violated McCavitt's reasonable expectation of privacy that he had in the personal information he stored on his computer hard drive.

In addition to establishing that the police executed a search within the meaning of property-based concepts, McCavitt demonstrates here that the police instituted a search under the U.S. Supreme Court's privacy-based Fourth Amendment framework. To invoke the protection of the Fourth Amendment under the privacy-based approach, the defendant must establish that he has an expectation of privacy in the place searched and that his expectation of privacy is legitimate. *Minnesota v. Carter*, 525 U.S. 83, 88 (1998); *Smith v. Maryland*, 442 U.S. 735, 740 (1979); *People v. Pitman*, 211 Ill. 2d 502, 514 (2004). The U.S. Supreme Court's approach embracing a privacy-based model traces its genesis to the concurring opinion of Justice Harlan in

Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan J. concurring). Justice Harlan's concurring opinion in *Katz* was first adopted by the full Court in *California v. Ciraolo*, 476 U.S. 207, 211 (1986) and reaffirmed in several cases, including *Carter* and *Smith*. To properly assert a legitimate expectation of privacy, the claim must be based on a "source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Byrd*, 138 S. Ct. at 1527 quoting *Rakas*, 439 U.S. at 144 n. 12; *Pitman*, 211 Ill. 2d at 514.

Here, McCavitt had a substantial interest in the privacy of his personal computer, the accompanying hard drive, and the personal information he stored digitally on the hard drive. (R10-12.) A person's expectation of privacy in the contents of his personal information stored on his computer is one that society recognizes as legitimate. The *McCavitt* Appellate Court majority found, "Individuals have a reasonable expectation of privacy in their personal computers and computer files." *McCavitt*, 2019 IL App (3d) 170830, ¶ 17; *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); *Guest v. Lee*, 255 F.3d 325, 333 (6th Cir. 2001) ("Home owners would of course have a reasonable expectation of privacy in their homes and in their belongings — including computers — inside the home."); *People v. Blair*, 321 Ill. App. 3d 373, 381-82 (3rd Dist. 2001) (Homer J. specially concurring) ("By placing information in computer files, a person manifests a reasonable expectation of privacy in the contents of those files.") Expansive privacy expectations are generated by computers and their hard drives because of the wide amount and scope of personal information stored on these electronic devices that is kept private from other persons. *See, e.g., United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007) ("A personal

computer is often a repository for private information the computer's owner does not intend to share with others.")

Courts have compared computer hard drives to homes as a core constitutionally protected area because of the degree and extent of personal information about the user's private lives that are kept in these receptacles. *See, e.g., United States v. Galpin*, 720 F.3d 436, 446 (2nd Cir. 2013) ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."); *see also*, *Ganias*, 755 F.3d at 135 (quoting *Galpin*). Because computers typically store vast amounts of private information, searches of computers entail a significant degree of intrusiveness. *United States v. Payton*, 573 F.3d 859, 861-62 (9th Cir. 2009). Thus, as in this case, a police-directed exploration of a person's hard drive for information related to criminal activity creates the potential for significant privacy violations. (R33.)

Property concepts also inform the privacy-based analysis. "One of the main rights attaching to property is the right to exclude others . . . and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude." *Byrd*, 138 S. Ct. at 1527 quoting *Rakas v. Illinois,* 439 U.S. 128 n. 12 (1978). Illustrating this principle, the Court stated: "One who owns and possesses a car, like one who owns and possesses a house, almost always has a reasonable expectation of privacy in it." *Id.* at 1527. By the same token, a person such as McCavitt who owns and possesses a computer and its hard drive that the police seized surely has a reasonable expectation of privacy in it. (R10-12.)

Feehan's examination of the mirrored hard drive violated McCavitt's reasonable expectation of privacy that he had in his personal computer, hard drive, and the personal

information stored in this electronic devise and thus was a Fourth Amendment search. By placing information in his computer files, McCavitt manifested an expectation of privacy in the contents that society would find reasonable. *See Blair*, 321 Ill. App. 3d at 381-82 (Homer J. specially concurring). In addition, McCavitt's digital files were password protected from unauthorized users trying to get access to his files, thus demonstrating additional expectations that his digital information would remain private. (R183.)

McCavitt's legitimate expectation of privacy in his personal information stored on his computer and hard drive is further reinforced by the U.S. Supreme Court's seminal decision in *Riley v. California*, 134 S. Ct. 2473 (2014). In *Riley*, the Court held that the police must obtain a warrant before searching a cell phone seized from a defendant during a search incident to arrest. *Id.* Glaringly absent from the State's brief is any discussion of *Riley*, one of the Court's most significant recent pronouncements on the Fourth Amendment's protections against encroachment on the substantial expectations of privacy that people have in their electronic devices.

Riley illuminates the nature and depth of McCavitt's expectation of privacy in his computer and accompanying hard drive. The Court in *Riley* identified the cell phone as a type of minicomputer, which this Court should find comparable to McCavitt's computer, hard drive, and its forensic exact duplicate in terms of the substantial, legitimate privacy expectations flowing from these electronic devices. *See id.* at 2489 (identifying cell phone as a mini-computer).

In *Riley*, the Court identified the cell phone as an electronic device that allows its user to store immense sums of personal data. The Court explained:

> The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

Id. Surely, the cell phone in *Riley* is substantially similar to McCavitt's hard drive insofar as the immense capacity of both to store huge amounts of varied private information over an extended period of time. *See United States v. Lichtenberger*, 786 F.3d 478, 488 (6th Cir. 2015) (noting *Riley's* recognition of the likelihood that an electronic device contains 1) many kinds of data, 2) in vast amounts, and 3) corresponding to a long swath of time.) As to the cell phone's storage capacity, the Court in *Riley* explained: "One of the most notable distinguishing features of modern cell phones is their immense storage capacity." *Riley*, 134 S. Ct at 2489. In another comment directed at the nearly ubiquitous presence of cell phones in the personal lives of their users: "[M]any of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives — from the mundane to the intimate." *Id.* at 2490.

The cell phone, the *Riley* Court stressed, is a broader and more extensive repository of intimate and casual personal information than even the home, which lies at the core of revered Fourth Amendment protections. *Id.* at 2491; *see People v. Bonilla*, 2018 IL 122484, ¶ 17 ("[T]he home has heightened expectations of privacy and at the core of the fourth amendment is the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.") (internal quotations omitted); *Id. at* ¶ 40 ([T]he home has heightened expectations of privacy.")

As the Court in *Riley* observed,

> [A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form — unless the phone is.

Riley, 134 S. Ct at 2491 (emphasis in original.)

The Court in *Riley* summarized the enormous privacy interests at stake for the ordinary person using a cell phone that stores the user's vast network of personal information:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life."

Id. at 2494-95. Our Illinois Appellate Court has logically extended the reasoning of *Riley*: "although *Riley* involved cell phones, the Supreme Court's comments are equally applicable to any modern computerized device that can store great quantities of data." *Carlson v. Jerousek*, 2016 IL App (2d) 151248, ¶ 45 n.2. The commonsense conclusion to be drawn from *Riley* is that the examination of "information stored on electronic devices can raise unique privacy concerns." *Id*. Applying *Riley* and its progeny here, this Court should determine that the police examination of McCavitt's exact duplicate hard drive for evidence of criminal activity is a substantial invasion of McCavitt's legitimate expectation of privacy and thus a search within the meaning of the Fourth Amendment. (R33.)

2. Feehan's examination of McCavitt's private, digital information on the mirrored hard drive is no less invasive than had he performed the examination on the original.

(Response to State's Brief at Part I.B.)

The State argues that McCavitt had either nonexistent or diminished privacy interests because Feehan conducted the examination on a forensic copy of the hard drive as opposed to the original. Therefore, according to the State, Feehan's examination of the forensic duplicate was not a Fourth Amendment search. (St. Br. at 17-23.) To the contrary, McCavitt's legitimate privacy expectations are no less compelling if his personal information stored on his hard drive is copied and preserved on an electronic device controlled by the police and then examined extensively for evidence of criminal activity. Far-reaching advances in technology enabling the

police or the government to forensically copy a person's electronic personal affairs into a mirrored hard drive, as was done to McCavitt (R22-26), does not extinguish his compelling Fourth Amendment justification for keeping his personal affairs private - whether that information is stored in his hard drive or its exact duplicate. Technological innovations do not render the Fourth Amendment a meaningless nullity.

As Professor Orin S. Kerr made clear in his seminal article on the Fourth Amendment's role in regulating computer searches: "*searches of copies should be treated the same as searches of the original."* (emphasis in the original). Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L. Rev. 531, 531 (2005). There is little, if any, practical difference between a new digital file and a copied version when evaluating the privacy interests at stake for the owner of that data. Professor Kerr explains:

> All computer data is a copy. Computer hard drives work by generating copies; accessing a file on a hard drive actually generates a copy of the file to be sent to the computer's central processor. More broadly, computers work by copying and recopying information from one section of the machine to another. From a technical perspective, it usually makes no sense to speak of having an `original' set of data. Given this, it would be troublesome and artificial to treat copies as different from originals.

Kerr, at 564. Stated another way, it is "unworkable, if not nonsensical, to treat copies of data as distinct from the so-called 'original'". Kerr at 564.

Although not a case involving the interference in a person's privacy caused by government-directed digital searches, the U.S. Supreme Court decision in *Church of Scientology of Cal. v. United States*, 506 U.S. 9 (1992) gave considerable weight to the privacy interests copies of documents have in the Fourth Amendment setting:

> [I]f the Government retains only copies of the disputed materials, a taxpayer still suffers injury by the Government's continued possession of those materials, namely, the affront to the taxpayer's privacy. A person's interest in maintaining the privacy of his `papers and effects' is of sufficient importance to merit constitutional protection.

Id. at 13.

Citing the Professor Kerr article, one court explained in painstaking detail what happens during a forensic search, as was done in the present case, and has spoken incisively about the far-ranging threat to privacy engendered by the government's forensic copying and then examining of an individual's hard drive copy. *See United States v. Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014). Forensic searches, the court observed, are inherently more invasive than an already invasive conventional computer search "A forensic search is a different procedure, fundamentally, from a conventional search. It occurs when a computer expert creates a bitstream copy and it analyzes it by means of specialized software." *Saboonchi*, 990 F. Supp. 2d at 569. "It is the potentially limitless duration and scope of a forensic search of the imaged contents of a digital device that distinguishes it from a conventional computer search." *Saboonchi*, 990 F. Supp. 2d at 561.

When a forensic search is undertaken:

> [A] computer forensics expert will use specialized software to comb through the data, often over the course of days, weeks, or even months, (*Kerr*) at 537-38, searching the full contents of the imaged hard drive, examining the properties of individual files, and probing the drive's unallocated 'slack space' to reveal deleted files, (Kerr) at 542-43. Although directed by a forensic examiner, an integral part of a forensic examination is the use of technology-assisted search methodology, where the computer searches vast amounts of data that would exceed the capacity of a human reviewer to examine in any reasonable amount of time. The techniques used during a forensic search can be distinguished from a conventional computer search, in which [the searcher] may operate or search an electronic device in much the same way that a typical user would use it.

Id. at 547; (R22-26.)

As another court explained, the owner of a personal computer has a significant privacy interest in keeping the original digital documents private and an identically protected privacy interest with respect to the imaged files. *United States. v. Metter*, 860 F. Supp. 2d 205, 212 (Dist.

Court E.D. NY 2012). The images or mirrored copies of the original document contain all the same information as the original document. *Id.* at 212. The long-term retention by police of the imaged digital documents trigger the owner's interest in preserving privacy to the same extent as it would for the original documents. *Id.*

Still another court has articulated eloquently on the need to erect barriers to far-reaching technological breakthroughs that threaten the integrity of privacy:

> Much has been written through the ages about why privacy is such an enduring value. The right to be left alone, to possess an inviolate zone of not just privacy but secrecy in some aspects of our lives, particularly from the coercive power of the State, is not less precious today than it was 100 years ago. It is instead much more urgent because of the extraordinary ease with which modern technology in an instant can pierce the most private confines of our lives.

Thompson, 51 Misc. 3d at 727. Remarking on the invasiveness of forensic searches, the Ninth Circuit Court of Appeals called a forensic search a "computer strip search" and stated that such a "thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity." *Cotterman*, 709 F.3d at 966, 968. Still, another court found that copying interferes with the owner's sole possession and interest in privacy of the information contained in his documents. *Jefferson*, 571 F. Supp. 2d at 703.

The U.S. Supreme Court in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) has warned about the pressure that ever more sophisticated technologies bear on the ability of ordinary citizens to live their private lives free from government encroachment. The *Carpenter* Court observed: "As Justice Brandeis explained in his famous dissent, the Court is obligated — as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government' — to ensure that the 'progress of science' does not erode Fourth Amendment

protections." *Id.* at 2223 citing *Olmstead v. United States*, 277 U.S. 438, 473-74 (1928) (Brandeis J. dissenting).

Neither McCavitt nor any citizen, present or future, can expect to keep sensitive, private affairs private if the government can have unfettered access to that information though a forensically manufactured duplicate and use this as a pretext to remove the Fourth Amendment as a bulwark protecting privacy. When the forensic copy is an exact duplicate of the original as it is here, it makes no substantive difference to the owner's prized right of privacy to say that the search was directed at the copy rather than the original since the copy is an exact duplicate of the original. To say that the government-engineered examination of an exact duplicate of an owner's hard drive is not a search implicating the Fourth Amendment merely because the object of the search is an exact duplicate created and possessed by the government would effectively allow technological innovations to extinguish the Fourth Amendment.

3. McCavitt did not have diminished privacy interests based on the particulars of his written motion for the return of his property following his acquittal on the sexual assault charges.

(Response to State's Brief at Part I.B.)

The State claims that McCavitt had a diminished expectation of privacy because he allegedly did not seek the return of the original hard drive or its copy in his written motion for the return of his property. (St. Br. at 17, 20.) In making this claim, however, the State neglects to acknowledge that McCavitt steadfastly asserted that he owned and possessed his desktop tower, personal computer and accompanying hard drive when the police seized it from his home. (R10.) McCavitt did not give permission to any law enforcement agency or the police to examine or search his computer or any of its contents. (R11-12.)

On March 19, 2014, the same day as McCavitt's acquittal on all charges in Case No. 13-CF-741, McCavitt, through his counsel, asked the trial court to direct the police to return all

items seized from him pursuant to the warrants, including his computer and hard drive, and the personal digital information contained therein. (R11-12.) Additionally, McCavitt filed a written motion for the return of his property. (A38.) In having asked for the return of his property in court the same day as his acquittal, McCavitt was prompt in seeking to protect his privacy and property interests. McCavitt's property has never been returned to him. (R11-12.)

Neither the State's brief nor its petition for leave to appeal (PLA) argued that McCavitt abandoned his property or privacy interest in the original or hard drive copy or the digital information contained therein. Thus, the State forfeited this claim. *See People v. Carter*, 208 Ill. 2d 309, 318 (2003) (State waived (now forfeiture) issue by repeatedly failing to raise issue in appellate court or its petition for leave to appeal with the Illinois Supreme Court).

Alternatively, on the merits, although a person who abandons property no longer has a privacy interest in it, McCavitt did not abandon his property, possessory, or privacy interests in his computer, the hard drive, the forensic duplicate or his private information contained in these devices. *People v. Pitman*, 211 Ill. 2d 502, 519-20 (2004). Whether property in a Fourth Amendment context has been abandoned is determined under a totality of the circumstances approach but with particular emphasis on explicit denials of ownership or relinquishment of property. *Id.* at 519-20.

Here, McCavitt affirmatively claimed ownership and possessory rights to his computer, and original hard drive and his personal information contained therein. (R11-12) He did not voluntarily relinquish possession over his property. McCavitt never told the police that they could keep his property or the hard drive duplicate or that he was giving them permission to conduct an invasive forensic search of his private affairs. Thus, contrary to the State's technical claim regarding the form of his motion for return of his property, McCavitt did not have

diminished property and privacy interests in his computer, the forensic duplicate or his personal information stored on these devices.

The State's cited authorities *United States v. Burgard*, 675 F.3d 1029 (7th Cir. 2012) and *People v. McGregory*, 2019 IL App (1st) 173101 shed no light on McCavitt's legitimate expectation of privacy calculus. (St. Br. at 20.) Both *Burgard* and *McGregory* addressed whether a prolonged delay between the seizure of a defendant's property and the obtaining of a search warrant was constitutionally unreasonable. By contrast, as shall be discussed in the next issue of this brief, the constitutional violation here was not the lesser infraction of mere delay in getting a warrant as in *Burgard* and *McGregory* but rather the search of McCavitt's digital information post-acquittal before obtaining a warrant authorizing the search. *See* Issue II *infra*. Moreover, *Burgard* and *McGregory* addressed only possessory interests affected by a prolonged seizure, not privacy interests violated from the search of a seized object as in the present case.

4. This Court should reject the State's "second look" claim that McCavitt had a reduced expectation of privacy.

(Response to State's Brief at Part A.1.)

The State's "second look" rationale that McCavitt had diminished privacy interests should be rejected for the reasons discussed in Issue II.5 *infra*

5. McCavitt has established a search under the privacy-based model and therefore is not required to show that his property rights were violated in order to show that the police performed a search.

Neither is McCavitt required to establish a search under the property-based construct for this Court to adopt his argument that Detective Feehan conducted a search under the privacy approach. "Expectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property, or on the invasion of such an interest." *Byrd*, 138 S. Ct. at 1526 quoting *Rakas v. Illinois*, 439 U.S. 128 n. 12 (1978). Property

concepts though not a required aspect of the analytical framework may nevertheless be instructive in determining whether privacy interests have been violated. *Id.* at 1526.

While privacy does not displace property, the flipside is also true: property does not displace privacy. The Court in *Carpenter v. United States*, 138 S. Ct. 2206, n. 1 (2018) held that while property interests may be informative in determining whether an expectation of privacy is legitimate, they are by no means "fundamental or "dispositive." *Id*. The Court further found that *Katz* rejected the proposition that property interests control whether a legitimate expectation of privacy can be established and that property rights do not cause the relevant privacy interests to rise or fall. *Id*. The U.S. Supreme Court has not overruled the privacy standard formulated in *Katz*. *See id*. Therefore, McCavitt has established a search because his reasonable expectation of privacy was violated, regardless of whether he has established that his property rights were infringed under the property rights Fourth Amendment approach. *See* Parts I.C. D. and E. *supra*.

E. Conclusion: Detective Feehan's examination of McCavitt's mirrored hard drive and discovery of digital images was a Fourth Amendment search.

McCavitt has established that the police conducted a Fourth Amendment search of his hard drive duplicate and the stored information on that device under both the property and privacy-based approaches. McCavitt next will show that the search was unreasonable.

II. Detective Feehan's search was unreasonable because he did not obtain a warrant before conducting the search following McCavitt's acquittal on the sexual assault charges.

A. The Fourth Amendment required Feehan to obtain a warrant because his search was directed to discovering evidence of criminal activity.

(Response to State's Brief at Part C.1.)

Without giving a reason why a warrant was not constitutionally necessary, the State claims that a balancing test should be applied to measure the reasonableness of the search. (St. Br. at 23-26.) This Court should firmly reject the State's invitation to apply an *ad hoc* balancing

test to determine whether the warrantless search was reasonable. The Fourth Amendment itself has already done its own balancing in favor of a warrant. "[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment — subject only to a few specifically established and well-delineated exceptions." *Arizona v. Gant*, 556 U.S. 332, 338 (2009); *People v. Cregan*, 2014 IL 113600, ¶ 25 ("Warrantless searches are *per se* unreasonable under the fourth amendment, subject to a few specific exceptions.")

Feehan was obligated to seek a warrant because his search entailed an investigation to turn up evidence of criminal behavior. The reasonableness of a particular type of search is initially assessed "by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests." *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 619 (1989) (citation omitted). In the realm of criminal cases, however, the Court most often strikes this balance in favor of the procedures to be followed under the Warrant Clause of the Fourth Amendment. *Skinner*, 489 U.S. at 619. Thus, "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing,… reasonableness generally requires the obtaining of a judicial warrant." *Riley* 134 S. Ct. at 2482, quoting *Vernonia School Dist., 47J v. Acton*, 515 U.S. 646, 653 (1995). "Warrantless searches are typically unreasonable" where the police undertake a search for the purpose of finding evidence of criminal conduct. *Carpenter*, 138 S. Ct. at 2221. Specifically rejecting a balancing approach for investigations of criminal wrongdoing, the Court in *Riley* found "the warrant requirement is an important working part of our machinery of government, not merely an inconvenience to be somehow 'weighed' against the claims of police efficiency." *Riley*, 134 S. Ct. at 2482.

Citing to the record of proceedings, the State's brief readily admits that the search of the duplicate hard drive was undertaken to investigate McCavitt's alleged participation in criminal activity other than the crimes listed in the original warrant. (St. Br. at 23-24 citing R32, 36-38, 40-41.) Paradoxically bolstering McCavitt's argument that a warrant was required but not secured, the State admits that the controlling reason for the police search here was that they suspected McCavitt of committing crimes in addition to the conduct that resulted in the charges for which he was acquitted. (St. Br. at 24.)

The State notes Feehan's explanation of the reason for the search: he suspected that his investigation would uncover other victims, leading to the prospect of additional charges that could be filed against McCavitt. (St. Br. at 24.) Indeed, the State concludes its discussion on this topic with the statement that "the PPD had a significant interest in determining whether its employee, a law enforcement officer, was participating in sexually based criminal conduct." (St. Br. at 24.) Applying *Riley, Carpente*r, and *Vernonia School Dist*. here, the Fourth Amendment required Feehan to secure a search warrant before he was authorized to investigate, examine and search for evidence on the duplicate hard drive-in order to connect McCavitt to criminal sexual activity.

Feehan's decision to conduct his search without judicial scrutiny removed a constitutionally-designed check on the powers of the police. The judiciary is interposed as an intermediary to curb unbridled police discretion that poses a threat to the citizenry's liberties. This takes the form of a neutral and detached magistrate empowered to decide whether the police have probable cause to conduct a search instead of the police officers themselves who lack impartiality because they are involved in the competitive enterprise of ferreting out crime. *See Riley*, 134 S. Ct. at 2482 citing *Johnson v. United States*, 333 U.S. 10, 14 (1932).

The State argues that the police had a significant interest in investigating alleged criminal sexual conduct. (St. Br. at 24-25.) The police, however, are not lawfully entitled to disregard the warrant requirement and jettison the protections of the Fourth Amendment, even if the alleged offense is especially serious. *See Mincey v. Arizona*, 437 U.S. 385, 393-94 (1978); *Carpenter*, 138 S. Ct. at 2265 (Gorsuch J. dissenting) (citing *Mincey*, "Our cases insist that the seriousness of the offense being investigated does *not* reduce Fourth Amendment protection.") (emphasis in the original); *People v. Faine*, 88 Ill. App. 3d 387, 389 (2nd Dist. 1980) (citing *Mincey* to reject the premise that the "seriousness of the offense under investigation itself creates exigent circumstances of the kind that under the fourth amendment justifies a warrantless search."); *People v. Lewis*, 75 Ill. App. 3d 259, 277 (1st Dist. 1979) (same).

B. Feehan's March 2014 post-acquittal search exceeded the probable cause justifications for the July 2013 warrants because the police directed their search to evidence of different crimes and different victims not covered by the warrants.

Feehan's post-acquittal search was unreasonable because it went beyond the probable cause justifications for the July 2013 warrants. The Fourth Amendment required Feehan to get a new warrant to search the forensic duplicate hard drive for evidence of additional crimes following McCavitt's acquittal of the criminal sexual assault charges that formed the basis for the warrants. The original July 2013 search warrants were limited to a single criminal sexual assault against a single complainant for which McCavitt was acquitted. Feehan's warrantless search a few days after McCavitt's acquittal was unreasonable because he expanded the course of his investigation to try to implicate McCavitt in other crimes that were not the subject of the original July 2013 warrants.

At the outset, the State has forfeited this issue by failing to argue at any point in these proceedings at the appellate, or Supreme Court level that Feehan's post--acquittal search was

within the scope of the July 2013 warrants or that getting an additional warrant was not constitutionally necessary. The *McCavitt* majority memorialized the State's concession:

> The State concedes that the July 17, 2013, warrant did not authorize Feehan's search, as that warrant had already been executed and, after investigation and criminal proceedings, defendant was acquitted.

McCavitt, ¶ 30. Neither in the State's petition for leave to appeal (PLA) nor in its brief to this Court does it challenge its own concession. The State fails to argue that the July 2013 warrants authorized the search. Rather, the State argues that an *ad hoc* balancing test should be employed to determine whether the search is reasonable. (St. Br. at 23-26.) Therefore, the State has forfeited the issue whether the July 2013 warrants authorized the search. *See People v. Carter*, 208 Ill. 2d 309, 318 (2003) (State waived (now forfeiture) issue by repeatedly failing to raise issue in appellate court or its petition for leave to appeal with the Illinois Supreme Court); *see* Ill. S. Ct. R. 341(h) (7) (eff. May 25, 2018) ("Points not argued are forfeited and shall not be raised.").

On the merits, this Court should determine that a new warrant was constitutionally required because the July 2013 warrants did not authorize Feehan's post-acquittal search. A warrant is "limited by the terms of its authorization." *Walter v. United States*, 447 U.S. 649, 656 (1980) (plurality opinion). "If the scope of the search exceeds that permitted by the terms of a validly issued warrant . . . , the subsequent seizure is unconstitutional without more." *Horton v. California*, 496 U.S. 128, 140 (1990); *United States v. Gimmett*, 439 F. 3d 1263, 1268 (10th Cir. 2006) ('law enforcement may not expand the scope of a search beyond its original justification."). "A search pursuant to a valid warrant may become an impermissible general search if . . . the police 'flagrant[ly] disregard . . . the limitations of [the] search warrant' and the search 'unreasonably exceeded the scope of the warrant.'" *United States v. Evers*, 669 F.3d 645,

652 (6th Cir. 2012) quoting in part *United States v. Garcia*, 496 F.3d 495, 507 (6th Cir. 2007). In such circumstances, the Fourth Amendment obligates the police to obtain another warrant to enable it to broaden its search beyond the scope of the first warrant to include crimes not covered by the first warrant. *United States v. Nasher-Alneam*, 399 F. Supp. 3d 579, 592 (S. D. W.Va. 2019); *People v. Raehal*, 401 P. 3d 117 ¶ 31 (Colo. App. 2017) (Generally, to search for evidence of a second crime, a second warrant is required).

Courts have held that the police violate the Fourth Amendment where they use a first warrant authorizing a search for a specific crime as a basis to search for evidence of other crimes without obtaining a second warrant. *See, e.g.*, *People v. Hughes*, No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020) (police violating the Fourth Amendment when they searched the defendant's cell phone for evidence of armed robbery without obtaining a new warrant where the phone was seized pursuant to a warrant authorizing the search of the phone's data for evidence of drug trafficking); *United States v. Hulscher*, 4-16-Cr-40070-01-KES, 2017 WL 657436, *2-3 (police required to get a second warrant to search for evidence of firearms offenses on defendant's cell phone where first warrant was limited to investigation of counterfeiting offenses; evidence suppressed); *Nasher-Alneam*, 399 F. Supp. 3d at 593-94 (same where first warrant was for violations of the Controlled Substances Act but search was directed at health care billing fraud; evidence suppressed); *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999) (police violating Fourth Amendment by searching for evidence of child pornography under a warrant authorizing a search for drug offenses; evidence suppressed); *United States v. Schlingloff*, 901 F. Supp. 2d 1101, 1106 (C.D. Ill. 2012) (police violating the Fourth Amendment by searching a computer under warrant for evidence of passport fraud and identity theft but

broadening the search to uncover child pornography without getting a second warrant; evidence suppressed).

In this case, the July 17, 2013 and July 24, 2013 warrants were based on a complaint and affidavit for search warrant from a police officer seeking authority to seize and examine certain digital media and other items from McCavitt's residence to investigate an alleged sexual assault based on a single incident that occurred against a single victim, whose name is A.K, on July 16, 2013 and July 17, 2013 respectively. (A16-17; A25-28.) The police officer alleged he had probable cause to seize and examine the digital media and other items described in the warrant application based on certain facts alleged in the complaints claiming to have shown a sexual assault against A.K. (A16-17; A25-28.)

The State's own brief and its citations to the record paradoxically support McCavitt's claim that Feehan's search exceeded the probable cause justifications for the July 2013 warrants. (St. Br. at 24.) The State's brief erroneously justifies Feehan's post-acquittal search by pointing to facts that the "PPD suspected defendant of committing criminal conduct in addition to the conduct that resulted in the charges for which he was acquitted." (St. Br. at 24 citing R36-38, 40-41.) However, the probable cause justification for the July 2013 warrants was limited to a single alleged criminal sexual assault against a single victim that occurred over the evening and mornings of July 16, 2013 and July 17, 2013. Pressing on with its error evidencing a warrantless search, the State observed that "Feehan explained that he 'knew there were other victims that could be identified that could lead to future criminal charges.'" (St. Br. at 24 citing R32.)

Continuing with his testimony, Feehan remarked that "[I]n the back of my mind, I knew that there was [sic] other victims that could be identified during the formal that would turn criminal." (R32.) Feehan identified the possibility of "identifying the other victims during our

internal investigation that possibility existed and then could ultimately come back to State's Attorney's Office for review and possible charges." (R38.) However, Feehan's search for evidence of multiple crimes committed against additional victims as part of an investigation initiated after McCavitt's March 2014 acquittal did not fall within the authority of the July 2013 warrants that were issued prior to the start of Feehan's post-acquittal investigation.

The judge who issued the July 2013 warrants did not have probable cause to issue warrants for child pornography at the time the warrant was issued. The probable cause justifications for the July 2013 warrants were for crimes related to a criminal sexual assault on a single victim for a single incident that occurred on July 16, 2013 and July 17, 2013. When Feehan launched his new investigation in March 2014 and search pursuant to that investigation he was not searching for evidence connected to the sexual incident that formed the basis for the July 2013 warrants. For the foregoing reasons, Feehan unconstitutionally failed to secure a warrant before beginning his post-acquittal search.

C. This Court should reject the State's "second look" claim that McCavitt had a reduced expectation of privacy.

(Response to State's Brief at Part A.1.)

The State's "second look" rationale argued that because of *United States v. Edwards*, 415 U.S. 800 (1974) and its progeny, including this Court's decision in *People v. Richards*, 94 Ill. 2d 92 (1983), McCavitt had a reduced expectation of privacy in his computer and hard drive because these items had already been lawfully seized and examined pursuant to the July 2013 warrants. (St. Br. at 12-15.) McCavitt has already firmly established that the State's "second look" analysis should be rejected under the property-rights approach because under that approach he is not required to establish that his expectation of privacy was violated. *See* Part I.F. *supra*.

As will be explained here, this Court should also reject the State's "second look" claim premised on *Edwards* for an additional two reasons: First, this case is not governed by *Edwards* because *Edwards* did not address warrant searches. Second, McCavitt's privacy interests did not diminish when the police conducted a warrantless search on the contents of the duplicate hard drive.

At issue in *Edwards* was whether the police were authorized to search clothing taken from an arrestee during his lawful arrest approximately 10 hours later at the police station. The Court found that the search incident to arrest doctrine allowed the police to search the arrestee's belongings at the police station for a reasonable period of time after the arrest. *Edwards*, 415 U.S. at 805-06. The search at the police station in *Edwards* was therefore reasonable.

The Court in *Edwards*, however, did not consider whether a suspect's reasonable expectation of privacy is diminished following the seizure and search of a suspect's belongings in the context of warranted searches. Neither *Edwards* nor its progeny considered the constitutional reasonableness of warrantless searches that exceed the probable cause justifications for the earlier-issued warrant. The recent decision of the unanimous Michigan Supreme Court in *People v. Hughes*, No. 159652 2020 WL 8022850 (Mich. Dec. 28, 2020) supports McCavitt's conclusion that *Edwards* does not apply in the setting of warranted searches. In *Hughes*, the court addressed whether the search of an item pursuant to a search warrant eliminates the suspect's reasonable expectation of privacy in that item under *Edwards*. *Id.* at *10-12. The court in *Hughes* held that "the issuance of a search warrant does not eliminate entirely one's reasonable expectation of privacy but only allows a search consistent with the scope of the warrant." *Id.* at *12.

The second distinguishing feature between *Edwards* and its progeny and this case is the *Edwards* line of cases did not involve digital searches. The U.S. Supreme Court's decision in *Riley v. California*, 134 S. Ct. 2473 (2014) involving the search of data contained in a cell phone governs the expectation of privacy calculus in this case rather than *Edwards*. *Riley* shows that McCavitt's expectation of privacy was not diminished when Feehan embarked on his post-acquittal search of the mirrored hard drive.

Riley rejected application of the search incident to arrest doctrine exception to the warrant requirement for cell phone searches. *Riley*, 134 S. Ct. at 2485. The Court in *Riley* held generally that police must obtain a warrant before conducting a search of the data on a cell phone even for cell phones seized during a lawful arrest. *Id*. The Court reasoned that when privacy-related concerns are weighty enough, the police are required to secure a warrant notwithstanding that the arrestee has diminished expectations of privacy. *Id.* at 2488. The Court also reasoned that the wide breath of private information stored on cell phones implicates substantial privacy interests. *Id.* at 2488-2491. Thus, the cell phone user does not lose his expectation of privacy in the digital contents of his cell phone upon his arrest. *See id*. "[A]lthough *Riley* involved cell phones, the Supreme Court's comments are equally applicable to any modern computerized device that can store great quantities of data." *Carlson v. Jerousek*, 2016 IL App (2d) 151248, ¶ 45 n.2.

The State's reading of *Edwards* that a suspect has diminished or nonexistent privacy expectations in his personal items seized during his lawful arrest does not apply with respect to searches of digital information in electronic devices. Digital searches are constitutionally different than searches of other objects. The second look doctrine does not apply in the context of digital searches because the user and owner of digital data stored on electronic device

maintains the reasonable expectation of privacy in his private digital information even if the device on which it is stored was lawfully seized.

The Michigan Supreme Court's *Hughes* decision reinforces *Riley's* undermining of the second look doctrine that the State derives from *Edwards*. The court in *Hughes* found that the *Edwards* line of cases is inapplicable to cell phone data because of the substantial privacy interests at stake for cell phones. *Hughes*, No. 159652 2020 WL 8022850 at *10. *Hughes* observed the following about *Riley*: "It is clear that under *Riley*, citizens maintain a reasonable expectation of privacy in their cell-phone data and this reasonable expectation of privacy does not altogether dissipate merely because a phone is seized during a lawful arrest." *Id.* at *9. The court in *Hughes* found that officers seizing digital data can only search the data as long as the search is consistent with the scope of the warrant. *Id.*

More broadly, this Court should reject the State's misguided understanding of *Edwards* as a case standing for reduced privacy expectations. *Hughes* supports the proposition that the principle to be drawn from *Edwards* is that a subsequent police station search of objects seized during a lawful arrest is a reasonable search, not that the arrestee's expectations of privacy in those objects are somehow reduced because of their initial seizure. The court in *Hughes* found that *Edwards* did not determine that a person's expectation of privacy in an object was extinguished or reduced by a seizure of the object during a lawful arrest. *Id.* at *10. Rather the point to be gleaned from *Edwards*, according to *Hughes*, is that a subsequent search at the police station of objects seized during the lawful arrest a short time period after the seizure is reasonable because it is grounded on a reasonable continuation of the police authority to search pursuant to the search incident to arrest doctrine. *See Id.*

The decision in *Edwards* itself, even if it not viewed through the prism of *Riley*, fails to support the State's claim that the lawful seizure of a suspect's property results in reduced privacy expectations. *Edwards* stands for the proposition that the question that the Court should address for warranted searches is whether the search subsequent to the seizure meets the demands of Fourth Amendment reasonableness. Thus, a "second look" of a suspect's digital data is reasonable only if the search is conducted pursuant to the limitations of the warrant. *See Id*.

Applying the reasonableness standard of *Edwards* to the present case, the State's second look analysis is inapposite. McCavitt's reasonable expectation of privacy in his computer and hard drive was not extinguished under *Edwards* merely because the police seized these items under a warrant. The object of Feehan's post-acquittal search was for evidence of different, additional crimes that were outside the scope of the warrants that resulted in McCavitt's acquittal on the charges that formed the basis for the warrants. Feehan's search untethered to the probable cause justifications of the original warrants was therefore unreasonable and violated the Fourth Amendment.

The State also attempts to justify Feehan's warrantless search by alleging there is evidence in the record suggesting (without proving) that McCavitt tried to delete or destroy incriminating evidence on his computer before allowing officers into his home to execute the July 2013 warrants. (St. Br. at 25.) McCavitt was not a threat to delete or destroy evidence. McCavitt had no access to his hard drive or its forensic duplicate when Feehan conducted his unconstitutional, warrantless search. The State's unjustifiable concerns do not excuse the failure of the police to obtain another warrant. *See United States v. Hulscher*, 4-16-Cr-40070-01-KES, (Feb. 10, 2017)(Magistrate decision) ("[o]btaining a second warrant would have been effortless

— the digital evidence was already in the possession of police, so there was no risk that Mr. Hulscher would destroy or hide the evidence.").

D. Feehan's warrantless search violated the Fourth Amendment, regardless of whether McCavitt's right to the return of his property is based on the Fourth Amendment.

(Response to State's Brief at Part C.2.)

The State argues that the police retention of McCavitt's property after his acquittal and the failure to return that property to McCavitt did not infringe on any of his Fourth Amendment interests. (St. Br. at 27-32.) The State's argument is non-responsive to the pertinent issues McCavitt raises in this appeal. The relevant question is not whether the owner's right to the return of property is based on the Fourth Amendment. What matters here is that the police violated the Fourth Amendment by failing to obtain a warrant to authorize its post-acquittal search of McCavitt's duplicate hard drive.

The State's reasoning is flawed because it confuses and commingles a seizure with a search. Contrary to the implications of the State's brief, a seizure is conceptually distinct from a search. A seizure of property occurs when the police conduct a "meaningful interference with an individual's possessory interests in that property." *Soldal v. Cook County, Illinois*, 506 U. S. 56, 63 (1992). A search, on the other hand, occurs when the police intrude on a person's reasonable expectation of privacy or trespass on a person or on the house, papers, or effects of that person. *Jardines*, 569 U.S. at 5.

The police infringe on the Fourth Amendment by undertaking an unreasonable search, even if they have not acted in violation of the Fourth Amendment by the manner in which they have retained a suspect's property. *See, e.g., Riley*, 134 S. Ct. at 2473 (warrantless search of cell phone unreasonable even though the phone was lawfully seized); *United States v. Jacobsen*, 466

U.S. 109, 114 (1984) ("Even when government agents may lawfully seize . . . a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package."); *United States v. Chadwick,* 433 U.S. 1, 13 n. 8 ("[T]he [lawful] seizure [of respondents' footlocker] did not diminish respondents' legitimate expectation that the footlocker's contents would remain private."); *Hughes* 2020 WL 8022850, at * 9 (relying on *Riley, Jacobsen,* and *Chadwick* and noting the differences between seizures and searches to hold that the seizure of the defendant's cell phone pursuant to a warrant did not eliminate his expectation of privacy in the digital data on his phone, thus requiring a second warrant to authorize the search). Applying these authorities to the present case leads to the following conclusion: regardless of whether the illegal police retention of McCavitt's computer, hard drive, and hard drive copy following McCavitt's acquittal was constitutional, the seizure did not diminish McCavitt's reasonable expectation of privacy and the police were still required under the Fourth Amendment to obtain an additional warrant before initiating the post-acquittal search.

E. The plain view doctrine did not authorize Feehan's search because he did not have a lawful right to start a search following McCavitt's acquittal.

(Response to State's Brief at Part A.2.)

The State argues that the plain view doctrine authorized its discovery of evidence not listed in the "first look" warrant. (St. Br. at 16.) The State, however, did not satisfy a crucial element of the plain view doctrine: Feehan did not have a lawful right to start a search after McCavitt's acquittal because he did not have a warrant. The plain view doctrine therefore did not authorize Feehan's search.

The U.S. Supreme Court has held that the plain view doctrine does not authorize a warrantless search when a warrant is required. As the Court stated in *Horton v. United States*,

496 U.S. 128 (1990): "It is, of course, an essential predicate to any valid warrantless seizure of incriminating evidence that the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed." *Id.* at 136. The Court elaborated on this principle: "This is simply a corollary of the familiar principle . . . that no amount of probable cause can justify a warrantless search or seizure absent exigent circumstances." *Id.* at 137 n. 7; *see also Texas v. Brown*, 460 U.S. 730, 738-39 (1979) ("Plain view is perhaps better understood, therefore, not as an independent exception to the Warrant Clause, but simply as an extension of whatever the prior justification for an officer's access to an object may be.").

For the reasons already stated, Feehan violated the Fourth Amendment by initiating an unlawful, warrantless search on McCavitt's duplicate hard drive post-acquittal. During his unlawful search, Feehan discovered two images of child pornography. (R33.) Feehan did not lawfully view and seize any child pornography digital images because he did not have lawful authority to initiate a warrantless search following McCavitt's acquittal. The plain view doctrine does not legalize Feehan's unconstitutional, warrantless search and seizure of child pornography because he did not have the authority to initiate a warrantless search.

The courts align with McCavitt on this issue. They have rejected the use of plain view as a basis to legally seize items in open view when the search itself that led to the discovery of the items was unreasonable because it was unlawfully conducted outside the authority of a warrant. *See, e.g.*, *United States v. Hulscher*, 4-16-Cr-40070-01-KES, 2017 WL 657436, * 3 (Officer's search of "the complete, unsegregated iPhone data lacked a sufficient justification. Thus, the plain view doctrine does not apply"); *Hughes supra* n. 25 (Mich. Sup. Ct.) (plain view doctrine did not apply because the officer's search violated the Fourth Amendment since "it was not reasonably directed at uncovering evidence of the criminal activities alleged in the warrant.");

United States v Gurczynski, 76 M.J. 381, 388 (2017) ("A prerequisite for the application of the plain view doctrine is that the law enforcement officers must have been conducting a lawful search when they stumbled upon evidence in plain view. As noted, the officers in this case were not [doing so] because the execution of the warrant was constitutionally unreasonable."); *United States v. Richardson,* 583 F. Supp. 2d 694, 716 (W.D. Pa. 2008) (plain view argument "fails because [officer] was within computer files he was not permitted to be in when he viewed the images.").

III. The evidence obtained from the unconstitutional search of McCavitt's forensic duplicate hard drive should be suppressed under the exclusionary rule.

A. The good faith exception to the exclusionary rule does not apply because Feehan's initiation of a warrantless search was akin to a general search of the type despised by the Framers.

Given that the police violated McCavitt's Fourth Amendment rights, the evidence obtained from the unconstitutional search should be suppressed under the exclusionary rule. "Generally, courts will not admit evidence obtained in violation of the fourth amendment." *Bonilla,* 2018 IL 122484 at ¶ 35. The primary purpose of this exclusionary rule is to deter future police misconduct in order to protect the right to be free from unreasonable searches and seizures. *Id*. Evidence is to be suppressed where the benefits of suppression outweigh its costs. *People v. Manzo,* 2018 IL 122761, ¶ 62. Here, Feehan's seizure of two images of child pornography and the subsequent incriminating evidence that was later seized as a result of that discovery should all be suppressed. (R 33.)

The State suggests that the good faith exception to the exclusionary rule applies. (St. Br. at 34-35.) However, the State bears the burden of proof to invoke the good faith exception. *People v. Turnage,* 162 Ill. 2d 299, 309, 313 (1994). "The good-faith exception to the exclusionary rule is a judicially created rule providing that evidence obtained in violation of a

defendant's fourth amendment rights will not be suppressed when police acted with an objectively reasonable good-faith belief that their conduct [was] lawful, or when their conduct involved only simple, isolated negligence." *Bonilla*, 2018 IL 122484 at ¶ 35 (citations and internal quotations omitted). As the State correctly points out, the good faith inquiry turns on "whether a reasonably well-trained officer would have known that the search was illegal in light of all of the circumstances." *Burns*, 2016 IL118973, ¶ 52 (internal quotation marks omitted) quoting *People v. LeFlore*, 2015 IL 116799, ¶ 25. Here, a reasonably well-trained officer standing in Feehan's shoes would not have initiated and conducted a warrantless post-acquittal search of McCavitt's private information stored on the duplicate hard drive. Therefore, the good faith exception is inapplicable in this case.

The good faith exception to the exclusionary rule embodied in *United States v. Leon*, 468 U.S. 897 (1984) does not apply to a Fourth Amendment violation stemming from a warrantless search that exceeds the authority of a warrant. The U.S. Supreme Court in *Leon* carved out a good faith exception to the exclusionary rule for an officer's objective good faith reliance on a warrant that ultimately was found to be unsupported by probable cause. Feehan's constitutional violation in this case was not that he relied on a defective warrant. Rather, Feehan violated the Fourth Amendment because his search exceeded the parameters of the warrant itself and required an additional warrant to authorize the search. *See United States v. Mowatt*, 513 F.3d 395, 405 (4th Cir. 2008) ((("The Leon exception does not apply here because Leon only prohibits penalizing officers for their good-faith reliance on magistrates' probable cause determinations.")

Police officers fail to comply with a search warrant in objective good faith if they expand the scope of their search beyond the terms of the warrant. *See, e.g., United States v. Fuccillo*, 808 F.2d 173, 177 (1st Cir. 1987) ("The good faith exception, therefore, will not be applied unless

the officers executing search warrants, at the very minimum, act within the scope of the warrants and abide by their terms."); *People v. McPhee*, 256 Ill. App. 3d 102, 110 (1st Dist. 1993); ("The police actions here do not fall within the *Leon* good faith exception, however, because the warrant at issue was not legally defective. The police had a valid warrant; they simply acted outside of its scope."); *Nasher-Alneam*, 399 F. Supp. 3d at 596 (constitutional error "was not with the warrant itself but, rather, the government's execution of that warrant.") As earlier discussed, Feehan's search for evidence of additional crimes outside the scope of the July 2013 warrants violated the Fourth Amendment.

For purposes of the exclusionary rule, Feehan's warrantless search is akin to the despised general warrants that the Framers sought to abolish with the passage of the Fourth Amendment. "The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.'" *Payton v. New York*, 445 U.S.573, 583 (1980). The Framers made the right to freedom from unreasonable searches and seizures explicit in the Fourth Amendment by eradicating the indignities and violations of privacy wrought by general warrants and warrantless searches that had infuriated the colonists to such an elevated degree that they fought a war of independence from England over these searches. *Byrd* 138 S. Ct. at 1526. In keeping with this historical tradition of antipathy toward general warrants and warrantless searches, the Court has guarded against police practices that permit its officers "unbridled discretion to rummage at will among a person's private effects." *Id.* quoting *Arizona v. Gant*, 556 U.S. 332, 345 (2009).

The rationale for blanket suppression here is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith becomes essentially a general warrant. *United States v. Liu*, 239 F.3d 138, 140-41 (2d Cir. 2000). Suppression is usually reserved for instances

where officers ignore the limitations of a general warrant and go on a fishing expedition to rummage through property for any indication of broad criminal activity. *United States v. Webster*, 809 F.3d 1158, 1165-66 (10th Cir. 2016) ("The basis for blanket suppression when a search warrant is executed with flagrant disregard of its terms is found in our traditional repugnance to 'general searches' which were conducted in the colonies pursuant to writs of assistance."); *United States v. Garcia*, 496 F.3d 495, 507 (6th Cir. 2007) (The remedy for a general search is suppression of all evidence obtained during the general search).

The warrantless search of McCavitt's mirrored hard drive on March 24, 2014, a few days after McCavitt's March 19, 2014 acquittal on sexual assault charges that formed the basis for the warrant is akin to the unchecked rummaging of a person's property in hopes of turning up evidence of crime that the Framers abhorred. (R29-33.) Feehan's post-acquittal search was to investigate his hunch that McCavitt had committed other crimes besides the criminal sexual assault that was the basis for the initial warrants. Feehan's warrantless, unchecked rummaging of McCavitt's private digital information for evidence of crimes was akin to the despised general search that calls for blanket suppression of all the evidence obtained as a result of the search.

This conclusion is bolstered by the fact that the probable cause justifications for the July 2013 warrants that led to the charges initially lodged against him and, of which, he later was acquitted. "A verdict of not guilty, whether rendered by the jury or directed by the trial judge, shields the defendant from a retrial for the same offense." *People v. Knaff*, 196 Ill. 2d 460, 468 (2001); *Tibbs v. Florida*, 457 U.S. 31, 41 (1982).

This principle shows that Feehan was not investigating McCavitt on the criminal sexual assault charge on which he was acquitted because the State could not retry McCavitt for the same offense. This self-evident fact demonstrates that Feehan knew he was investigating McCavitt

post-acquittal for additional offenses that were beyond the scope of the original warrant that was limited to an offense on which McCavitt been acquitted. Thus, Feehan's sweeping warrantless search beyond the reach of the original warrant was an intentional or reckless act, not just simple negligence, and mandates blanket suppression. *See, e.g.*, *Hulscher*, 2017 WL 657436, *2-3 (evidence suppressed as a result of police failure to obtain a second warrant before embarking on an expanded search beyond the probable cause justifications of the original warrant); *Nasher-Alneam*, 399 F. Supp. 3d at 593-94 (same); *Carey*, 172 F.3d at 1276 (10th Cir. 1999) (same); *Schlingloff*, 901 F. Supp. 2d at 1106 (C.D. Ill. 2012) (same).

Another reason why Feehan cannot demonstrate objective good faith is his testimony showing that he knew McCavitt was acquitted of the criminal sexual assault charges that formed the basis for the probable cause justifications for the warrants. (R29-33.) Once Feehan knew of the acquittal and knew that he was expanding his investigation beyond the scope of the acquitted charge to include a widened probe of other additional crime victims and uncharged crimes that he suspected McCavitt of committing, a reasonably well-trained officer acting in objective good faith would have sought another warrant before starting the search. Feehan's failure to do so was in flagrant disregard of core Fourth Amendment principles condemning general warrants and unchecked rummaging. Suppression is necessary to deter officers from expanding searches to cover possible crimes and crime victims on which a judicial officer has not made a probable cause determination. Application of the exclusionary rule would encourage officers to obtain a warrant supporting a probable cause basis for the search. For the foregoing reasons, this Court should affirm the appellate court's order suppressing the State's evidence.

IV. McCavitt's convictions should be reversed outright without remand for a new trial or further proceedings.

With the incriminating evidence of child pornography seized from the mirrored hard drive suppressed, the State does not have sufficient evidence to obtain a conviction based on proof beyond a reasonable doubt. Because the State is unable to prevail absent the suppressed evidence, this Court should reverse McCavitt's convictions outright without remand for a new trial. *See, e.g., People v. Blair*, 321 Ill. App. 3d 373; 380-81 (3d Dist. 2001) (reversing conviction outright where there was insufficient evidence to convict without the suppressed evidence); *People v. Abdur-Rahim*, 2014 IL App (3d) 130588, ¶ 33 (same).

CONCLUSION

Wherefore, the Defendant-Appellee John T. McCavitt respectfully requests this Honorable Court affirm the appellate court's reversal of the trial court's order denying the defendant's motion to suppress evidence. This Court should uphold the suppression of the State's evidence seized from McCavitt's computer, hard drive, and mirrored hard drive, including but not limited to any and all images of child pornography. With the evidence suppressed, this Court should reverse McCavitt's convictions for child pornography outright and vacate his sentence or in the alternative reverse the conviction and remand for further proceedings.

Respectfully submitted,

/s/ Joshua B. Kutnick

JOSHUA B. KUTNICK
Attorney for Defendant-Appellee

/s/ James K. Leven

JAMES K. LEVEN
Attorney for Defendant-Appellee

CERTIFICATE OF COMPLIANCE

I certify that the defendant-appellee's response brief conforms to the requirements of Rules 341(a) and (b). The length of this response brief, excluding the pages containing the Rule 341(d) cover, the Rule 341(h)(1) statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 50 pages.

/s/ Joshua B. Kutnick

JOSHUA B. KUTNICK
Attorney for Defendant-Appellee
900 West Jackson Blvd., Ste. 7E
Chicago, IL 60607, 312-441-0211
joshua@kutnicklaw.com

/s/ James K. Leven

JAMES K. LEVEN
Attorney for Defendant-Appellee
203 North LaSalle Street, Ste. 2100
Chicago, IL 60601, 312-558-1638
jameskleven@attorneyleven.com

No. 125550

IN THE
SUPREME COURT OF THE STATE OF ILLINOIS

THE PEOPLE OF THE STATE OF ILLINOIS Plaintiff-Appellant	)	Appeal from the Appellate Court of Illinois, Third District, No. 3-17-0830
vs.	)	There on appeal from the Circuit Court of the Tenth Judicial Circuit, Peoria County, Illinois No. 14 CF 282
JOHN T. McCAVITT Defendant-Appellee	)	Honorable David Brown & Albert Purham Judges Presiding

PROOF OF SERVICE AND NOTICE OF FILING

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct. On **March 3, 2021**, the foregoing **Response Brief of Defendant-Appellee** was (1) filed with the Clerk of the Supreme Court of Illinois using the Court's electronic filing system, and (2) served by transmitting a copy from my email address to the email addresses of the persons named below. Additionally, upon its acceptance by the court's electronic filing system, the undersigned will send 5 copies of the **Response Brief of Defendant-Appellee** to the Clerk of the Supreme Court.

Respectfully Submitted,

/s/ Joshua B. Kutnick

Attorney for Defendant-Appellee

900 West Jackson Blvd., Ste. 7E

Chicago, IL 60607

312-441-0211

joshua@kutnicklaw.com

Kwame Raoul, Attorney General

Leah Bendik

Assistant Attorney General

100 W. Randolph St., 12th Floor

Chicago, IL 60601

Eserve.criminalappeals@atg.state.il.us

Thomas Arado

Deputy Director

Justin Nicolosi

Staff Attorney

State's Attorneys Appellate Prosecutor

3rddistrct.eserve@ilsaap.org

Hon. Jodi Hoos

Peoria County State's Attorney

JHoos@peoriacounty.org

James K. Leven

Attorney for Defendant-Appellee
203 North LaSalle Street, Ste. 2100

Chicago, IL 60601, 312-558-1638
jameskleven@attorneyleven.com

Brett Max Kaufman

Nathan Freed Wessler

American Civil Liberties Union Foundation

125 Broad Street

New York, NY 10004

212-549-2500

bkaufman@aclu.org

Counsel for Amici Curiae

Jennifer Stisa Granick

American Civil Liberties Union Foundation

39 Drumm Street

San Francisco, CA 94111

Counsel for Amici Curiae

Rebecca Glenberg

Nusrat J. Choudhury

Roger Baldwin Foundation of the ACLU of Illinois

150 N. Michigan Ave., Ste. 600

Chicago, IL 60602

Counsel for Amici Curiae