

2021 IL 125550

**IN THE  
SUPREME COURT  
OF  
THE STATE OF ILLINOIS**

---

(Docket No. 125550)

THE PEOPLE OF THE STATE OF ILLINOIS, Appellant, v.  
JOHN T. McCAVITT, Appellee.

*Opinion filed October 21, 2021.*

JUSTICE MICHAEL J. BURKE delivered the judgment of the court, with opinion.

Chief Justice Anne M. Burke and Justices Garman, Theis, Overstreet, and Carter concurred in the judgment and opinion.

Justice Neville dissented, with opinion.

**OPINION**

¶ 1 The Illinois State Police obtained warrants to seize and search a personal computer owned by defendant, John T. McCavitt, an officer of the Peoria Police Department. The warrant at issue in this appeal authorized law enforcement to

search the computer for digital evidence of two unrelated incidents: the aggravated criminal sexual assault of a named victim and the unauthorized video recording and live video transmission of an unnamed victim. Defendant was tried and acquitted of the alleged sexual assault before the unauthorized video recording was investigated.

¶ 2 Following defendant's acquittal and without seeking a new warrant, the Peoria Police Department acquired and searched a copy of the computer's hard drive, uncovering evidence of the unauthorized video recording. The digital search also uncovered child pornography, which was not mentioned in the warrant.

¶ 3 Based on the images, defendant was convicted of several counts of child pornography. The appellate court reversed the judgment on the ground that the search violated the fourth amendment (U.S. Const., amend. IV). 2019 IL App (3d) 170830, ¶ 32.

¶ 4 This appeal concerns the extent to which defendant's acquittal in the sexual assault proceedings affected his expectation of privacy in his computer data and whether the fourth amendment required the police to obtain a new warrant before searching the same data for evidence of another crime. The outcome turns on the interplay of four concepts: (1) a person's reasonable expectation of privacy in data on an electronic storage device that is subject to search, (2) double jeopardy principles, (3) the fourth amendment's particularity requirement as applied to electronic storage devices, and (4) the plain view doctrine.

¶ 5 In *People v. Hughes*, 958 N.W.2d 98, 104 (Mich. 2020) (*en banc*), the Michigan Supreme Court cogently explained that a search of an electronic storage device pursuant to a warrant must be reasonably directed at obtaining evidence relevant to the criminal activity alleged in the warrant. A search of digital data that is directed instead at uncovering evidence of criminal activity not identified in the warrant is effectively a warrantless search that violates the fourth amendment absent some exception to the warrant requirement. *Id.*

¶ 6 The warrant at issue diminished defendant's reasonable expectation of privacy in the images and videos he stored on his computer. When defendant was acquitted of the sexual assault, his reasonable expectation of privacy in his data relating to that offense was restored. However, the acquittal did not resolve the portion of the

warrant that authorized a search for digital evidence of the unauthorized video recording. The post-acquittal computer examination was reasonably directed at obtaining evidence of the unauthorized video recording, and the child pornography that was uncovered during the search was admissible because the images were found in plain view.

¶ 7 We hold that, under the unique facts of this case, the search that uncovered the child pornography did not violate defendant's fourth amendment rights. Therefore, we affirm the circuit's court's order denying defendant's motion to suppress the images and reverse the appellate court's judgment reversing that order.

## ¶ 8 I. BACKGROUND

¶ 9 This appeal is part of a series of three criminal prosecutions against defendant. All three are based on incriminating images and video uncovered on defendant's computer.

¶ 10 Defendant was charged in Peoria County case No. 13-CF-741 with aggravated criminal sexual assault (720 ILCS 5/11-1.30(a)(4) (West 2012)) and criminal sexual assault (*id.* § 11-1.20(a)(1)). Following defendant's acquittal in that case, the Peoria Police Department launched an internal investigation of defendant, which led to the discovery of additional incriminating images and video. The investigation was suspended when defendant was charged. He was ultimately convicted of (1) the unauthorized video recording of two women (Peoria County case No. 14-CF-203) and (2) child pornography in this case (Peoria County case No. 14-CF-282).

### ¶ 11 A. Peoria County Case No. 13-CF-741

¶ 12 Initially, defendant was investigated for criminal sexual assault against A.K., a female houseguest who was a friend and coworker of defendant's live-in girlfriend, Rachel Broquard. On July 17, 2013, the Illinois State Police obtained a warrant to search defendant's home for evidence of the alleged sexual assault, which defendant did not challenge.

¶ 13 The complaint for the warrant described A.K.'s account of the events. A.K. reported that defendant sexually assaulted her around 6 a.m. that day. A.K.,

Broquard, and defendant had gone out the previous night to celebrate with another coworker who was departing for graduate school. At approximately 4 a.m., A.K., Broquard, and defendant arrived at his residence and continued socializing. At 5:15 a.m., A.K. lay down, fully clothed, under the covers of a bed in a guest bedroom. A short time later, she awoke facedown wearing only her bra, which was pushed up. A.K. was in four-point restraints, and a black sleeping mask covered her head. She heard a “snap” that she believed to be from the cap of a lubricant container. A.K. also heard clicking noises that sounded like a camera shutter. Defendant sexually penetrated A.K. repeatedly and then released her from the restraints. A.K. quickly dressed, left the residence, and reported the incident.

¶ 14 The search warrant complaint alleged that digital evidence of criminal sexual assault could be found on defendant’s cellular phone. Accordingly, the warrant authorized the seizure of “any electronic media cable [*sic*] of video/audio recording” and “any electronic storage media capable of stor[ing] pictures, audio or video.” The warrant also authorized the seizure of any restraints that might have been used on the victim, physical evidence resulting from the assault, and any additional items of evidentiary value.

¶ 15 Officers of the Illinois State Police and the Peoria Police Department arrived at defendant’s home around 8:30 p.m. to execute the warrant. They waited two hours for defendant to answer the door and allow them inside. Defendant had called in sick to the police department that evening and had ignored telephone calls from his supervisors and the investigators. Defendant allegedly told Broquard that, while he kept the officers waiting outside, he removed the four-point restraints from the guest bedroom and placed them back under the mattress in the master bedroom.

¶ 16 The police officers seized defendant’s iPhone and his custom-built computer tower. The iPhone was found locked in a gun safe in the basement. The computer’s file history showed that more than 16,500 files had been recently deleted from the hard drive. The officers seized the restraints, a black blindfold, and lubricant. They also found a video recording system hidden inside two Kleenex tissue boxes.

¶ 17 An initial examination of the computer hard drive revealed photographs and video of A.K. lying motionless, facedown in four-point restraints. She was wearing only her top, which was pulled up, and a pillow covered her head. The officers

determined that the photographs and video of A.K. had been transferred from defendant's iPhone to his computer.

¶ 18 The initial examination of the hard drive also revealed what appeared to be secretly recorded video from defendant's bathroom of an unidentified woman stepping out of the shower. Defendant has not alleged that this initial examination of his computer data was unlawful.

¶ 19 On July 24, 2013, the Illinois State Police obtained a second warrant, which defendant also did not challenge. The warrant authorized "all peace officers in the state of Illinois" to search the computer for "any and all digital images, including, but not limited to JPG, GIF, TIF, AVI, MOV, and MPEG files" and "any evidence of" the offenses of (1) aggravated criminal sexual assault, (2) unlawful restraint, and (3) unauthorized video recording and live video transmission. The warrant authorized a search of "any and all stored/deleted data to determine which particular files are evidence or instrumentalities of criminal activity."

¶ 20 The search warrant complaint restated A.K.'s account of the events on July 17, 2013, but A.K. was not the only victim mentioned. The complaint specifically alleged that "[a]dditionally recovered videos display an unidentified female using the bathroom and taking a shower. The female appears to have no knowledge she was being recorded." Accordingly, the warrant authorized the search of defendant's computer for any evidence of the crimes listed "that may be discovered from separate incidents."

¶ 21 Detective Jeff Avery, a computer forensics expert with the Peoria County Sheriff's Department, examined defendant's computer. He removed the hard drive and made an exact, unalterable digital copy of its contents using EnCase software. Avery saved the copy, called the EnCase file, to his work computer. Avery reinstalled the hard drive and returned defendant's computer to the Illinois State Police.

¶ 22 Avery searched the EnCase file and found images relating to the incident involving A.K. On August 6, 2013, based on the images, the State charged defendant in Peoria County case No. 13-CF-741 with aggravated criminal sexual assault (720 ILCS 5/11-1.30(a)(4) (West 2012)) and criminal sexual assault (*id.*

§ 11-1.20(a)(1)) of A.K.<sup>1</sup> A jury ultimately found him not guilty of all charges on March 19, 2014.

¶ 23 Immediately following the not guilty verdicts, defense counsel orally requested the return of defendant's personal property. Counsel specifically mentioned "collector guns" but did not ask for the computer. The trial court deferred ruling and asked counsel to file a written motion, because the seized items were weapons.

¶ 24 B. Internal Investigation of Defendant

¶ 25 The next day, on March 20, 2014, the Peoria Police Department initiated a formal investigation of defendant.<sup>2</sup> Detective James Feehan, a computer forensics examiner with the police department, requested and received a copy of the EnCase file from Avery.

¶ 26 On March 24, 2014, Feehan began a digital forensic analysis of the EnCase file and uncovered two images of what he believed to be child pornography. He also found video recordings of two unidentified women using the bathroom in defendant's home. Feehan suspended his search to apply for a new warrant to further examine the EnCase file for child pornography.

¶ 27 Also on March 24, 2014, defendant filed a written motion in Peoria County case No. 13-CF-741, the sexual assault case, requesting the return of his property. The motion was silent as to the legal basis for the proposed disposition of defendant's property. On April 24, 2014, the court ordered the return of defendant's "guns + weapons instantan" but otherwise continued the motion. The motion was never fully resolved, and defendant's computer was not returned.

¶ 28 C. Peoria County Case No. 14-CF-203

¶ 29 On March 28, 2014, defendant was arrested and charged in Peoria County case No. 14-CF-203 with two counts of unauthorized video recording (720 ILCS 5/26-

---

<sup>1</sup>The July 24, 2013, warrant authorized a search for evidence of unlawful restraint—presumably committed against A.K.—but defendant was not charged with the offense.

<sup>2</sup>An arbitrator's ruling and the police department's collective bargaining agreement prohibited an internal investigation of defendant while the criminal case was pending.

4(a) (West 2014)) based on two incidents unrelated to the sexual assault charges. The pending criminal charges caused the Peoria Police Department to suspend its internal investigation of defendant.

¶ 30 The charges were based on the video recordings of two women, identified as Rachel G. and Whitney S., who were acquaintances of defendant and Broquard. *People v. McCavitt*, 2021 IL App (3d) 180399-U, ¶¶ 8-9. Defendant, using cameras concealed in the Kleenex boxes, secretly recorded the women using his bathroom. Defendant recorded Rachel on March 27, 2013, and recorded Whitney sometime between May 1, 2013, and the date his computer was seized.<sup>3</sup> Defendant transferred the video files to his computer.

¶ 31 D. Peoria County Case No. 14-CF-282

¶ 32 On April 1, 2014, Feehan obtained the new warrant to search the EnCase file for additional images of child pornography, which he uncovered soon thereafter. On April 28, 2014, the State filed a 10-count indictment, charging defendant with 7 counts of aggravated child pornography (720 ILCS 5/11-20.1B (West 2010)), a Class 2 felony, and 3 counts of child pornography (720 ILCS 5/11-20.1 (West 2012)), a Class 3 felony, based on five images found in the EnCase file.

¶ 33 On August 15, 2014, defendant filed a motion to suppress, arguing that Feehan had no authority to obtain and examine the contents of the EnCase file in March 2014. Defendant asserted that Feehan's examination was a warrantless search in violation of the fourth amendment because no criminal charges were pending at the time of the search. He also claimed the trial court in Peoria County case No. 13-CF-741, the sexual assault case, had erroneously failed to order the return of his computer and all copies of the hard drive, pursuant to section 108-2 of the Code of Criminal Procedure of 1963. See 725 ILCS 5/108-2 (West 2012).

¶ 34 Feehan testified at the suppression hearing that, as soon as he discovered the two pornographic images, he stopped to apply for a search warrant. He explained

---

<sup>3</sup>The State elected to prosecute the child pornography case first, but defendant ultimately was convicted of the two counts of unauthorized video recording. Defendant's convictions were affirmed on direct appeal. *McCavitt*, 2021 IL App (3d) 180399-U.

that the application process “took a couple days because we were investigating other unlawful videotaping evidence as part of that internal investigation.” On April 1, 2014, after obtaining the new warrant, Feehan resumed his search of the EnCase file and began looking specifically for child pornography.

¶ 35 Feehan testified that defendant had used White Canyon WipeDrive software, a utility program for permanently deleting data from a hard drive, at 9:23 p.m. on July 13, 2017, while the officers waited outside his home. However, Feehan was able to reconstruct how defendant had used the computer to search, download, and view child pornography from the Internet. Feehan referred to defendant’s work schedule to explain that defendant accessed the child pornography when he was off duty. Feehan recovered the file names of several permanently deleted images and videos that were labeled with child pornography acronyms, such as “PTHC,” meaning preteen hard core. Feehan was able to recover other files and identified their contents as child pornography.

¶ 36 Feehan pieced together the events during the hours between the alleged sexual assault and the computer seizure. Defendant called in sick to the police department at 6:01 p.m. Broquard used the computer for about 10 minutes, switched it off at 6:18 p.m., and went to work. At 6:26 p.m., defendant logged on as “owner,” and around 8:15 p.m. the police began knocking on defendant’s front door. Defendant deleted data from the computer from 9:18 p.m. to 10:07 p.m. Defendant allowed the police to enter around 10:30 p.m., at which time they seized the computer. Defendant was charged for the images that Feehan found despite defendant’s attempt to delete them permanently.

¶ 37 On cross-examination, Feehan testified that the Illinois State Police excluded him from the initial criminal investigation of the sexual assault to avoid a potential conflict of interest arising from Feehan and defendant sharing the same employer. Feehan conceded that he knew defendant had been acquitted of the sexual assault charges on March 19, 2014, and that no other charges were pending when he received the EnCase file from Avery on March 21, 2014. Feehan confirmed that he requested the EnCase file as part of the internal investigation even though he knew defendant’s computer had been seized in connection with the sexual assault prosecution.



¶ 38        Feehan testified, however, that at the time of his search, he “knew that there was [*sic*] other victims that could be identified during the formal [investigation] that would turn criminal.” Feehan did not believe he needed a search warrant or other court order to obtain and search the EnCase file “[b]ecause of case law that [he] was aware of” since defendant’s computer was previously seized “[p]ursuant to a lawful search warrant.”

¶ 39        On October 21, 2014, the trial court denied defendant’s motion to suppress, finding that law enforcement’s retention of defendant’s computer after the acquittal did not compel suppression of the child pornography. The court noted that defendant had not challenged (1) the warrants issued on July 17 and July 24, 2013, (2) the original search and seizure of his computer, or (3) Avery’s creation of the EnCase file. Regardless of whether the trial court in the sexual assault proceedings erred in failing to order the return of the computer, defendant had tried in that case to invoke section 108-2 of the Code of Criminal Procedure and had not alleged a fourth amendment violation. Moreover, returning the computer to defendant would not have prevented a search of the EnCase file, which Avery still possessed and had made available to Feehan. The trial court concluded that defendant’s suppression motion had raised an issue of search, not seizure. The seizure was presumptively reasonable because it was conducted pursuant to an unchallenged warrant, long before Feehan searched the EnCase file.

¶ 40        The trial court concluded that, once the police had the right to copy and examine the hard drive for evidence of certain crimes, defendant’s reasonable expectation of privacy in the information was substantially diminished but not totally frustrated. “[A]lthough the police had the right to search the hard drive for certain types of files and for evidence of certain types of offenses, the police did not have cart [*sic*] blanche to review everything on the hard drive.” For instance, the court noted, defendant still might have held expectations of privacy in a diary, daily planner, family history, drafts of papers for classes, and the like, but “he no longer held a ‘reasonable’ expectation of privacy in the types of files and directories which were or could be related to evidence of unlawful restraint and/or improper videotaping.”

¶ 41        The trial court found that Feehan did not violate defendant’s fourth amendment rights. Feehan’s search of files and folders for images and video did not exceed the scope of the original warrant because there was no testimony that the first two

images of child pornography were of a different file type or in different areas or directories of the computer than those previously subject to search under the warrant.

¶ 42 On July 10, 2015, the State amended its indictment and charged defendant with seven additional counts of child pornography (720 ILCS 5/11-20.1(a)(6) (West 2014)), a Class 2 felony, based on seven additional images found in the EnCase file.

¶ 43 A jury found defendant guilty of 15 of the 17 counts of child pornography. Defendant filed posttrial motions, which the trial court denied. The trial court accepted the jury's verdict on 1 count of Class 3 felony child pornography and 10 counts of Class 2 felony child pornography. The court sentenced defendant on the Class 3 felony to five years' imprisonment followed by mandatory supervised release of three years to life. The court imposed a sentence of 48 months' probation on the remaining 10 counts, to be served consecutively to the prison sentence.

¶ 44 On direct appeal, defendant argued, *inter alia*, that the trial court erroneously denied his motion to suppress. He argued that "Feehan's search of his EnCase file eight months after the initial warrant was issued and following his acquittal of sexual assault charges violated his fourth amendment rights." 2019 IL App (3d) 170830, ¶ 13. The Appellate Court, Third District, agreed and reversed the convictions.

¶ 45 The majority opinion concluded that, when the police took possession of defendant's computer, his expectation of privacy was significantly diminished until his sexual assault acquittal, which then triggered a statutory right to the return of his property and restored his expectation of privacy in the computer. *Id.* ¶ 24. The majority held that, although Avery created the EnCase file lawfully, Feehan violated defendant's right to privacy when he searched the file and found the first two images of child pornography. *Id.* ¶ 25. The police were not entitled to retain the entire EnCase file indefinitely but could examine it and retain only those files within the scope of the initial warrant. The majority held that, once defendant's sexual assault trial ended, the police were not entitled to retain any portion of the EnCase file, much less the entire file. *Id.* The majority concluded that, because the police had no authority to retain the EnCase file after defendant's acquittal, Feehan's initial search violated defendant's fourth amendment rights. *Id.* ¶ 26.

¶ 46 The majority also held that the images were not admissible under the good-faith exception to the exclusionary rule. *Id.* ¶ 31. Feehan, who had been a police officer for more than 20 years and a forensic examiner for 17 years, knew when he requested the EnCase file that defendant had been acquitted of the sexual assault charges and that no new charges had been filed. The majority concluded that, because the charges based on the files found pursuant to the initial warrant were no longer pending, Feehan should have known that the police had no right to retain, much less search, the EnCase file. *Id.* We note the majority opinion did not address the portion of the search warrant concerning the separate incident of unauthorized video recording.

¶ 47 The dissenting opinion concluded that defendant's acquittal did not entitle him to the immediate return of his computer or the information harvested from it. *Id.* ¶ 37 (Wright, J., dissenting). The dissent noted that, after the acquittal, defendant did not pursue his oral and written requests for the return of his property. *Id.* ¶ 39. The dissent characterized the sexual assault court's deferral of the oral request as a denial and concluded that the ruling stands as the law of the case and represents an unappealable order. *Id.* ¶ 40. The dissent also concluded that, because Feehan was merely reviewing information that had already been lawfully seized by another detective who had made it a part of his working file, defendant's reasonable expectation of privacy remained diminished after he lawfully lost possession of the computer tower pursuant to the search warrant. *Id.* ¶ 44.

¶ 48 The State petitioned for leave to appeal, which we allowed pursuant to Illinois Supreme Court Rule 315(a) (eff. Oct. 1, 2019). We granted the American Civil Liberties Union and the American Civil Liberties Union of Illinois leave to submit briefs *amicus curiae* in support of defendant's position, pursuant to Illinois Supreme Court Rule 345 (eff. Sept. 20, 2010).

¶ 49

## II. ANALYSIS

¶ 50 On appeal, the State argues Feehan's examination of the EnCase file did not violate defendant's fourth amendment rights because the search arose from the original lawful seizure and search of his computer. The State characterizes the search as a permissible "second look" that was no broader than the "first look" authorized by the original search warrant, which was broadly written,

unchallenged, and presumptively valid. The State also contends defendant's privacy and possessory interests in the EnCase file were so significantly reduced by the sexual assault prosecution that Feehan's examination did not even constitute a "search" under the fourth amendment. Third, the State asserts that, even if Feehan's examination qualifies as a warrantless search, the officer's review was reasonable because it constituted, at most, a minimal intrusion on defendant's privacy and possessory interests while diligently promoting compelling law enforcement interests. The State alternatively contends that the child pornography was admissible under the good-faith exception to the exclusionary rule.

¶ 51 Defendant renews his arguments that the child pornography should have been suppressed because Feehan's examination was a search that violated his expectation of privacy under the fourth amendment and that the images are not admissible under the good-faith exception to the exclusionary rule. Defendant also argues his property interest in the computer conferred a reasonable expectation of privacy in the data at the time of Feehan's search.

¶ 52 A. Standard of Review

¶ 53 We apply our familiar two-part standard of review to a ruling on a suppression motion. First, the circuit court's findings of historical fact should be reviewed only for clear error, and a reviewing court must give due weight to any inferences drawn from those facts by the fact finder. *People v. Luedemann*, 222 Ill. 2d 530, 542 (2006) (citing *Ornelas v. United States*, 517 U.S. 690, 699 (1996)). We defer to the court's factual findings and will reverse those findings only if they are against the manifest weight of the evidence. *Id.* (citing *People v. Sorenson*, 196 Ill. 2d 425, 431 (2001)). Second, a reviewing court may undertake its own assessment of the facts as they relate to the issues and may draw its own conclusions when deciding what relief should be granted. *Id.* (citing *People v. Pitman*, 211 Ill. 2d 502, 512 (2004)). Accordingly, the circuit court's ultimate legal ruling on the suppression motion is reviewed *de novo*. *Id.* As the relevant facts in this case are not in dispute, our review of the suppression ruling is *de novo*.

¶ 54

## B. Fourth Amendment

¶ 55

Defendant argued in his motion to suppress that Feehan's examination violated his rights under the fourth amendment of the United States Constitution and article I, section 6, of the Illinois Constitution of 1970. The fourth amendment to the United States Constitution protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., amend. IV; see also *Elkins v. United States*, 364 U.S. 206, 213 (1960) (the fourth amendment applies to state officials through the fourteenth amendment (U.S. Const., amend. XIV)). Similarly, article I, section 6, of the Illinois Constitution provides that the "people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches [and] seizures." Ill. Const. 1970, art. I, § 6; see also 725 ILCS 5/108-7 (West 2012) (requiring the place or person to be searched and the items to be seized to be "particularly described in the warrant"). Under our limited lockstep doctrine, we construe the search and seizure clause of our state constitution in accordance with the United States Supreme Court's interpretation of the fourth amendment unless any of the narrow exceptions to lockstep interpretation apply. *People v. Holmes*, 2017 IL 120407, ¶ 24. Defendant does not argue that an exception applies here.

¶ 56

The fourth amendment contains two separate clauses: the reasonableness clause and the warrant clause. U.S. Const., amend. IV; *Kentucky v. King*, 563 U.S. 452, 459 (2011). The reasonableness clause requires that all government searches and seizures be reasonable. *King*, 563 U.S. at 459; *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006) (the touchstone of fourth amendment analysis always is "reasonableness"). The warrant clause permits courts to issue warrants only if (1) the warrant is supported by probable cause and (2) the warrant includes particularized descriptions of "the place to be searched" and "the persons or things to be seized." U.S. Const., amend. IV; *King*, 563 U.S. at 459. The second condition of the warrant clause is known as the particularity requirement.

¶ 57

A search warrant is not always required before searching or seizing a citizen's personal effects (see *Stuart*, 547 U.S. at 403), but there is a "strong preference for searches conducted pursuant to a warrant" (*Illinois v. Gates*, 462 U.S. 213, 236 (1983)), and police officers generally must obtain a warrant for a search to be reasonable under the fourth amendment (see, e.g., *Riley v. California*, 573 U.S. 373,

382 (2014); *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (searches conducted outside the judicial process, without prior approval by a judge or magistrate, are *per se* unreasonable under the fourth amendment, subject only to a few specifically established and well-delineated exceptions).

¶ 58 C. Reasonable Expectation of Privacy in Digital Information

¶ 59 A search is constitutional if it does not violate a person’s “reasonable” or “legitimate” expectation of privacy. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). To claim protection under the fourth amendment, a person must have exhibited an actual subjective expectation of privacy in the place searched or thing seized, and this expectation must be one that society is willing to recognize as reasonable. *People v. Rosenberg*, 213 Ill. 2d 69, 77 (2004). As in most cases, this appeal concerns whether defendant’s actual expectation of privacy was objectively reasonable.

¶ 60 There is no bright line rule indicating whether an expectation of privacy is constitutionally reasonable. See *O’Connor v. Ortega*, 480 U.S. 709, 715 (1987). Whether a defendant has a legitimate expectation of privacy in the place searched or the property seized thus depends on factors including (1) property ownership, (2) whether the defendant was legitimately present in the area searched, (3) the defendant’s possessory interest in the area searched or the property seized, (4) prior use of the area searched or property seized, (5) the ability to control or exclude others’ use of the property, and (6) a subjective expectation of privacy in the property. *People v. Lindsey*, 2020 IL 124289, ¶ 40. Whether a person’s expectation of privacy in an area searched is legitimate is determined by an objective standard drawn from common experience and based on the totality of the circumstances. *Id.*

¶ 61 In the context of the fourth amendment, computers and other electronic storage devices have historically been viewed as closed containers. Because individuals generally retain a reasonable expectation of privacy in the contents of a closed container that conceals its contents from plain view (see *United States v. Ross*, 456 U.S. 798, 822-23 (1982)), they also generally retain a reasonable expectation of privacy in data stored on electronic devices.

¶ 62        Accessing information stored in an electronic storage device will implicate the owner’s reasonable expectation of privacy in the information. *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (an individual generally has a reasonable expectation of privacy in their personal computers and data files). For instance, in *Riley*, the Supreme Court of the United States held that law enforcement generally must obtain a warrant before conducting a search of cell phone data. *Riley*, 573 U.S. at 386. The court described cell phones as “minicomputers that also happen to have the capacity to be used as telephones.” *Id.* at 393. Cell phones and personal computers share the notable distinguishing features of immense storage capacity and the ability to collect many distinct types of information, including a user’s Internet browsing history and “a cache of sensitive personal information” concerning nearly every aspect of a person’s life. *Id.* at 393-95.

“[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.” (Emphasis omitted.) *Id.* at 396-97.

As the cell phone privacy concerns expressed in *Riley* apply to personal computers, we conclude that Feehan’s examination of the EnCase file constituted a search under the fourth amendment.

¶ 63        The State cites *United States v. Edwards*, 415 U.S. 800 (1974), for the proposition that the valid “first look” diminished defendant’s expectation of privacy and permitted Feehan’s examination. *Edwards* held that, when a person is lawfully arrested and taken into custody, the items in his possession when arrested—which were lawfully subject to search at the time and place of his arrest—may also be lawfully searched and seized without a warrant even though a “substantial period of time” has elapsed between the arrest and the time that the items are later searched. *Id.* at 807. *Edwards* does not apply because all the searches in this case were purportedly conducted pursuant to a warrant, not incident to defendant’s arrest. Furthermore, *Riley* instructs that law enforcement generally must obtain a warrant to search data on an electronic storage device, even if it was seized incident to arrest.

¶ 64

#### D. Defendant's Expectation of Privacy

¶ 65

Although an individual retains a reasonable expectation of privacy in a computer under his control, special circumstances may affect that expectation. In this case, the trial court correctly observed that defendant did not challenge the warrants authorizing the seizure of his computer, Avery's creation of the EnCase file, or Avery's subsequent search for digital evidence of the sexual assault. The unchallenged warrants made the initial seizure and search of defendant's computer presumptively reasonable.

¶ 66

Defendant, however, challenges Feehan's initial examination of the EnCase file, which uncovered evidence of the two incidents of unauthorized video recording and two images of child pornography. The State argues that Feehan's examination was not even a "search" under the fourth amendment because the initial warrant diminished defendant's privacy and possessory interests. In support, the State points out that the item searched was not the original hard drive but a copy that Avery created and stored on his work computer. The State asserts defendant did not have a legitimate expectation of privacy in the EnCase file because he did not create, own, or have lawful access to it. See *Lindsey*, 2020 IL 124289, ¶ 42.

¶ 67

The State focuses on defendant's lack of a formal property interest in the EnCase file itself and disregards defendant's informal privacy interest in his personal data. Defendant persuasively argues that "Feehan's examination of the police-generated forensic copy of [defendant'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." The right to exclude others is one of the main rights attaching to property, and allowing access to a copy defeats that right. See *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978); see also *United States v. Jefferson*, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008) ("the Fourth Amendment protects an individual's possessory interest in information itself," and copying interferes with the owner's possession and interest in privacy of the information contained in the documents).

¶ 68

The evidentiary value of data resides in the data itself, not in the medium on which it is stored. To suggest that defendant lacked an expectation of privacy in the contents of his personal computer because those contents were copied to another medium contravenes the requirement of reasonableness, which is the touchstone of



any fourth amendment analysis. See *Stuart*, 547 U.S. at 403. “[I]maging a computer should be regulated by the Fourth Amendment and searches of copies should be treated the same as searches of the original” (Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 532 (2005)) because “computers work by copying and recopying information” (*id.* at 564). Treating a digital copy as the original recognizes that the key to fourth-amendment reasonableness is the access to data, regardless of whether the data is copied, transferred, or otherwise manipulated. *Id.*

¶ 69 We agree with defendant that his privacy interest in the computer’s contents extended to the EnCase file. But he goes further, asserting his property interest in the data obviates the need to show an expectation of privacy. He claims “[h]e 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.” Defendant’s property interest in the data is not dispositive of the search’s reasonableness, otherwise mere proof of ownership in a place or item to be searched would be sufficient for suppression.

¶ 70 To summarize, defendant’s privacy interests in the original hard drive and the EnCase file were the same. However, the privacy interest conferred by his ownership of the computer is not dispositive to our inquiry. The appeal turns on defendant’s privacy interest in light of the warrant and the reasonableness of Feehan’s examination of the EnCase file following defendant’s acquittal in the sexual assault proceeding.

¶ 71 E. Restoration of Defendant’s Expectation of Privacy

¶ 72 Defendant argues that, once he was acquitted in the sexual assault case, (1) he was entitled by statute to the return of his property, (2) his expectation of privacy in the computer was restored, and (3) it was unreasonable for law enforcement to look at the data without obtaining a new warrant. We conclude that defendant’s acquittal only partially restored his reasonable expectation of privacy in his computer.

¶ 73

## 1. Criminal Sexual Assault

¶ 74

The parties do not dispute that defendant's sexual assault trial culminated in an acquittal for double jeopardy purposes. An acquittal triggers the double jeopardy clause of the fifth amendment to the United States Constitution, which provides that no person shall "be subject for the same offence to be twice put in jeopardy of life or limb." U.S. Const., amend. V. Similarly, article I, section 10, of the Illinois Constitution provides that no person shall "be twice put in jeopardy for the same offense." Ill. Const. 1970, art. I, § 10. The prohibition against double jeopardy is animated by the principle that

" 'the State with all its resources and power should not be allowed to make repeated attempts to convict an individual for an alleged offense, thereby subjecting him to embarrassment, expense and ordeal and compelling him to live in a continuing state of anxiety and insecurity, as well as enhancing the possibility that even though innocent he may be found guilty.' " *People v. Williams*, 188 Ill. 2d 293, 307 (1999) (quoting *Green v. United States*, 355 U.S. 184, 187-88 (1957)).

¶ 75

"The prohibition against double jeopardy 'protects against three distinct abuses: (1) a second prosecution for the same offense after acquittal; (2) a second prosecution for the same offense after conviction; and (3) multiple punishments for the same offense.' " *People v. Henry*, 204 Ill. 2d 267, 283 (2003) (quoting *People v. Placek*, 184 Ill. 2d 370, 376-77 (1998)); see also *United States v. Wilson*, 420 U.S. 332, 343 (1975). "An acquittal triggers the bar against double jeopardy only if the acquittal 'actually represents a resolution, correct or not, of some or all of the factual elements of the offense charged.' " *Henry*, 204 Ill. 2d at 283 (quoting *United States v. Martin Linen Supply Co.*, 430 U.S. 564, 571 (1977)).

¶ 76

When the jury found defendant not guilty of aggravated criminal sexual assault and criminal sexual assault, the verdicts represented a resolution of the factual elements of the offenses charged. The bar against double jeopardy protected defendant against a second prosecution for those offenses, restoring defendant's reasonable expectation of privacy concerning the data that constituted evidence of those crimes. Defendant, newly freed from "a continuing state of anxiety and insecurity" that he would be retried for sexual assault (*Williams*, 188 Ill. 2d at 307),

regained a reasonable expectation that the police would not search his computer for evidence of the offenses of which he was acquitted.

¶ 77 Defendant renews his argument that the acquittal entitled him to the return of his computer and to any copies of his personal data and that therefore his reasonable expectation of privacy in the data was restored *entirely*. We disagree. To establish a legitimate expectation in the place to be searched, a defendant must point to a source outside the constitution—namely, formal property interests or informal privacy interests. *United States v. Jones*, 565 U.S. 400, 408 (2012); *Rakas*, 439 U.S. at 143 n.12 (“Legitimation of expectations of privacy by law must have 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.”).

¶ 78 Defendant asserts his formal property interests in the computer, relying on section 108-2 of the Code of Criminal Procedure, which governs the return of property after a person is released from custody. But the statute applies to items seized *without* a warrant, stating

“An inventory of all instruments, articles or things *seized on a search without warrant* shall be given to the person arrested and a copy thereof delivered to the judge before whom the person arrested is taken, and thereafter, such instruments, articles or things shall be handled and disposed of in accordance with Sections 108-11 and 108-12 of this Code. If the person arrested is released without a charge being preferred against him all instruments, articles or things seized, other than contraband, shall be returned to him upon release.” (Emphasis added.) 725 ILCS 5/108-2 (West 2012).

¶ 79 Section 108-2 arguably did not apply to defendant’s computer because the statute applies to “things seized without a warrant.” Defendant’s acquittal does not negate the fact that the defendant’s computer was seized on July 17, 2013, pursuant to a warrant.

¶ 80 In contrast to section 108-2, section 108-10 applies to items seized *with* a warrant, like defendant’s computer. Section 108-10 provides for the items seized by law enforcement to be returned to the court:

“A return of all instruments, articles or things seized shall be made without unnecessary delay before the judge *issuing the warrant* or before any judge *named in the warrant* or before any court of competent jurisdiction. An inventory of any instruments, articles or things seized shall be filed with the return and signed under oath by the officer or person *executing the warrant*. The judge shall upon request deliver a copy of the inventory to the person from whom or from whose premises the instruments, articles or things were taken and to the *applicant for the warrant*.” (Emphases added.) *Id.* § 108-10.

¶ 81 Regardless of which statute governed the custody of defendant’s computer, we agree with the trial court and the dissenting appellate opinion that defendant failed to invoke any authority for the return of his computer or copies of its hard drive. In fact, defendant states in his brief that his “items have never been returned,” but he does not accuse the State of any wrongdoing.

¶ 82 Moreover, defendant cites no authority to suggest that his acquittal automatically entitled him to the immediate return of his computer and the information harvested from it. In fact, section 108-11 provides that “[t]he court before which the instruments, articles or things are returned shall enter an order providing for their custody pending further proceedings.” *Id.* § 108-11. Thus, the statute contemplates a motion and a hearing before an order is entered disposing of seized items. See, e.g., *City of Chicago v. Pudlo*, 123 Ill. App. 3d 337, 345 (1983) (order denying defendants’ motion for return of weapons was reversed because trial court erroneously failed to conduct hearing). Here, the State argued at the suppression hearing that, if defendant had noticed up his motion, the State would have opposed the return of the computer to defendant on the ground that the hard drive contained contraband. In any event, the record indicates that defendant neither pursued his written motion for the return of his computer nor appealed any order in Peoria County case No. 13-CF-741.

¶ 83 Defendant asserts a possessory interest in the computer and claims it extends to the digital copies of the hard drive, but the trial court never reached the issue, which was governed by statute and was subject to an evidentiary hearing. As defendant did not press his rights in the sexual assault proceeding, he cannot claim his property interest fully restored his expectation of privacy in his data.

¶ 84

## 2. Unauthorized Video Recording

¶ 85

The acquittal resolved the portion of the July 24, 2013, search warrant that was directed toward the offense of aggravated criminal sexual assault. However, the acquittal did not resolve any of the factual elements of unauthorized video recording, which was also specified in the warrant. Contrary to defendant's suggestion, the acquittal did not nullify the warrant entirely. The State concludes that the sexual assault acquittal did not restore defendant's expectation of privacy concerning evidence of the uncharged offenses described in the July 24, 2013, warrant, including unauthorized video recording.

¶ 86

Defendant responds that the State has forfeited the issue. *Village of Lake Villa v. Stokovich*, 211 Ill. 2d 106, 121 (2004) (issues not raised in the trial court generally are forfeited and may not be raised for the first time on appeal). Defendant cites the appellate majority's observation that "[t]he 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.' " (Emphasis added.) 2019 IL App (3d) 170830, ¶ 30. But the State has argued throughout the proceedings that the *July 24, 2013*, warrant authorized Feehan's search.

¶ 87

For instance, the State argues in its opening brief that it had an ongoing interest in investigating defendant because, "based on prior searches of defendant's computer data, phone data, and email account, the [Peoria Police Department] suspected defendant of committing criminal conduct in addition to the conduct that resulted in the charges for which he was acquitted." The State narrows its argument in the reply brief, asserting that the search warrant described "separate incidents" besides the sexual assault of A.K. We consider the issue adequately preserved. *Dillon v. Evanston Hospital*, 199 Ill. 2d 483, 504-05 (2002) (the forfeiture rule is an admonition to the parties and not a limitation on the jurisdiction of this court).

¶ 88

## F. Scope of the Warrant

¶ 89

The validity of Feehan's search depends on whether it was within the scope of the portion of the warrant that was unresolved by the acquittal. It is well established that a search warrant need not contain " '[a] minute and detailed description of the

property to be seized.’ ” *People v. McCarty*, 223 Ill. 2d 109, 151 (2006) (quoting *People v. Prall*, 314 Ill. 518, 523 (1924)). “Rather, ‘the property must be so definitely described that the officer making the search will not seize the wrong property.’ ” *Id.* (quoting *Prall*, 314 Ill. at 523). When a type of property, rather than particular property, is to be seized, a description of its characteristics is sufficient. *Id.* at 152.

¶ 90 The Michigan Supreme Court has recently explained how the fourth amendment’s particularity requirement applies to digital evidence. In *Hughes*, the defendant was under investigation for drug trafficking, and law enforcement obtained a warrant to search his cell phone for evidence related to separate criminal allegations of that crime. *Hughes*, 958 N.W.2d at 105. The warrant affidavit contained no information concerning armed robbery. *Id.* The warrant provided that “ ‘[a]ny cell phones or \*\*\* other devices capable of digital or electronic storage seized by authority of this search warrant shall be permitted to be forensically searched and or manually searched, and any data that is able to be retrieved there from shall be preserved and recorded.’ ” *Id.* The warrant authorized the seizure of any drug paraphernalia and “ ‘any records pertaining to the receipt, possession and sale or distribution of controlled substances including but not limited to documents, video tapes, computer disks, computer hard drives, and computer peripherals.’ ” (Emphasis omitted.) *Id.* at 106.

¶ 91 After the cell phone was seized, the defendant was charged with an armed robbery that occurred a week before the warrant was issued. *Id.* The police examined the phone and extracted all the data. About a month after the extraction and at the request of the prosecutor in the armed-robbery case, a detective searched the cell-phone data again. *Id.* The searches uncovered evidence of the defendant’s involvement in the armed robbery, and the evidence was used to convict the defendant of armed robbery. *Id.* at 106-07.

¶ 92 On appeal from the armed-robbery conviction, the defendant argued that “the phone records should have been excluded from trial because the warrant supporting a search of the data only authorized a search for evidence of drug trafficking and not armed robbery.” *Id.* at 107. The Michigan Supreme Court agreed, concluding that the seizure and search of cell-phone data pursuant to a warrant does not

extinguish the “otherwise reasonable expectation of privacy in the entirety of that seized data.” *Id.* at 111. Specifically, the *Hughes* court held

“the police were permitted to seize and search that data, but only to the extent authorized by the warrant. Any further review of the data beyond the scope of that warrant constitutes a search that is presumptively invalid under the Fourth Amendment, absent some exception to that amendment’s warrant requirement.” *Id.* at 115.

¶ 93 The *Hughes* court then considered “whether the review of [the] defendant’s data for evidence of an armed robbery fell within the scope of the warrant issued in the drug-trafficking case.” *Id.* The court held that a search of cell-phone data “must be ‘reasonably directed at uncovering’ evidence of the criminal activity alleged in the warrant and that any search that is not so directed but is directed instead toward finding evidence of other and unrelated criminal activity is beyond the scope of the warrant.” (Emphasis omitted.) *Id.* (quoting *United States v. Loera*, 923 F.3d 907, 917 (10th Cir. 2019)).

¶ 94 The court acknowledged that a “criminal suspect will not always store or organize incriminating information on his or her digital devices in the most obvious way or in a manner that facilitates the location of that information.” *Id.* at 117. Nonetheless, the court declined

“to adopt a rule that it is always reasonable for an officer to review the entirety of the digital data seized pursuant to a warrant on the basis of the mere possibility that evidence may conceivably be found anywhere on the device or that evidence might be concealed, mislabeled, or manipulated.” *Id.*

¶ 95 “Such a per se rule would effectively nullify the particularity requirement of the Fourth Amendment in the context of cell-phone data and rehabilitate an impermissible general warrant that ‘would in effect give “police officers unbridled discretion to rummage at will among a person’s private effects.” ’ ” (Emphasis omitted.) *Id.* at 118 (quoting *Riley*, 573 U.S. at 399, quoting *Gant*, 556 U.S. at 345). An officer’s search of seized digital data, as with any other search conducted pursuant to a warrant, must be reasonably directed at finding evidence of the criminal activity identified within the warrant. *Id.*

¶ 96

The *Hughes* court explained that the test in the digital context is whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant. *Id.* Whether a data search that uncovers evidence of criminal activity not identified in the warrant was reasonably directed at finding evidence relating to the criminal activity alleged in the warrant turns on a number of considerations, including (1) the nature of the criminal activity alleged and the type of digital data likely to contain evidence relevant to the alleged activity; (2) the evidence provided in the warrant affidavit for establishing probable cause that the alleged criminal acts have occurred; (3) whether nonresponsive files are segregated from responsive files on the device; (4) the timing of the search in relation to the issuance of the warrant and the trial for the alleged criminal acts; (5) the technology available to allow officers to sort data likely to contain evidence related to the criminal activity alleged in the warrant from data not likely to contain such evidence without viewing the contents of the unresponsive data and the limitations of this technology; (6) the nature of the digital device being searched; (7) the type and breadth of the search protocol employed; (8) whether there are any indications that the data has been concealed, mislabeled, or manipulated to hide evidence relevant to the criminal activity alleged in the warrant, such as when metadata is deleted or when data is encrypted; and (9) whether, after reviewing a certain number of a particular type of data, it becomes clear that certain types of files are not likely to contain evidence related to the criminal activity alleged in the warrant. *Id.* at 118-20.

“To be clear, a court will generally need to engage in such a ‘totality-of-circumstances’ analysis to determine whether a search of digital data was reasonably directed toward finding evidence of the criminal activities alleged in the warrant only if, while searching digital data pursuant to a warrant for one crime, officers discover evidence of a different crime without having obtained a second warrant and a prosecutor seeks to use that evidence at a subsequent criminal prosecution.” *Id.* at 120.

¶ 97

The *Hughes* court found the search for armed robbery evidence was outside the scope of the warrant, which authorized a data search only for evidence of drug trafficking and “did not even mention” the armed robbery or its surrounding circumstances. *Id.* at 121. The second search of the phone violated the fourth amendment because the “review was directed exclusively toward finding evidence



related to the armed-robbery charge, and it was grounded in information obtained during investigation into that crime.” (Emphasis omitted.) *Id.* at 122.

¶ 98 We are persuaded by *Hughes* that an officer’s search of seized digital data, as with any other search with a warrant, must be reasonably directed at finding evidence of the criminal activity identified within the warrant.

¶ 99 The warrants in this case and in *Hughes* make the cases factually distinguishable. The *Hughes* warrant authorized a data search for evidence of drug trafficking, but the supporting affidavit did not mention armed robbery, let alone claim probable cause that the defendant committed armed robbery. As a result, the warrant did not authorize a search for digital evidence related to the armed robbery.

¶ 100 By contrast, the search warrant in this case was not limited to uncovering evidence of the sexual assault of which defendant was acquitted. The July 24, 2013, warrant also authorized a search for digital evidence of unauthorized video recording. Double jeopardy protected defendant from retrial on the sex offenses, but defendant still could be charged with unauthorized video recording, because the issuing court found there was probable cause to search defendant’s data for evidence of that offense.

¶ 101 The *Hughes* factors indicate Feehan’s search was reasonably directed at finding evidence of the unauthorized video recording. Specifically, the complaint for the July 24, 2013, search warrant stated that “[a]dditionally recovered videos display an unidentified female using the bathroom and taking a shower” and that this “unidentified female appears to have no knowledge she was being recorded.” The complaint expressly targeted the crime of “Unauthorized Video Recording/Live Video Transmission in violation of 720 ILCS 5/26-4,” and the warrant authorized the search of all digital images for “Unauthorized Video Recording/Live Video Transmission 720 ILCS 5/26-4.”

¶ 102 The warrant permitted a search of “any and all digital images, including, but not limited to JPG, GIF, TIF, AVI, MOV, and MPEG files,” which are image and video file formats likely to contain evidence relevant to unauthorized video recording. Moreover, the evidence provided in the search warrant application described the bathroom video in sufficient detail to establish probable cause. Defendant has not challenged Feehan’s methodology concerning search protocols

and the sorting of responsive and unresponsive data, and Feehan testified to defendant's attempts to hide relevant evidence by permanently deleting files. See *Hughes*, 958 N.W.2d at 118.

¶ 103 The concurring opinion in *Hughes* stated that an officer's subjective intention in conducting the search also should be considered as a potentially dispositive factor in determining whether the search of seized data is reasonably directed at finding evidence of the criminal activity identified in the warrant. *Id.* at 124 (Viviano, J., concurring). The concurrence concluded that, if the officer purposefully searches for evidence of a crime other than the one identified in the warrant, the search cannot be reasonably directed at uncovering evidence of the criminal activity alleged in the warrant. *Id.* at 124-25.

¶ 104 Feehan's conduct adhered to the special concurrence in *Hughes*. Feehan testified at the suppression hearing that he was not searching for evidence of the criminal sexual assault, because defendant already had been acquitted of that charge. But contrary to defendant's assertion, the detective did not engage in a fishing expedition. Feehan testified that "we were investigating other unlawful videotaping evidence as part of [the] internal investigation" and that he "knew that there was [*sic*] other victims" besides A.K. Also, Feehan actually uncovered evidence of the offense described in the warrant. The July 24, 2013, warrant authorized law enforcement to search for digital evidence of the unauthorized video recording of another victim, and Feehan's search and subjective intent were consistent with the warrant.

¶ 105 G. Timeliness of Search

¶ 106 Defendant primarily argues that his acquittal restored his expectation of privacy in all the data, but he also suggests that Feehan's search was unreasonable because it was conducted eight months after the warrant was issued. Following the acquittal, the warrant still authorized a search for evidence of unauthorized video recording, and as the appellate majority noted, the fourth amendment does not place explicit limits on the duration of any forensic analysis authorized by a warrant. 2019 IL App (3d) 170830, ¶ 19 (" 'under current law there is no established upper limit as to when the government must review seized electronic data to determine whether the

evidence seized falls within the scope of a warrant.’ ” (quoting *United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012))).

¶ 107 Courts have upheld forensic analyses begun months after law enforcement acquires the electronic storage device. See *United States v. Syphers*, 426 F.3d 461, 469 (1st Cir. 2005) (a five-month delay in processing a computer already in police custody “did not invalidate the search \*\*\* because there is no showing that the delay caused a lapse in probable cause, that it created prejudice to the defendant, or that federal or state officers acted in bad faith to circumvent federal requirements”); *United States v. Burns*, No. 07 CR 556, 2008 WL 4542990, at \*8-9 (N.D. Ill. Apr. 29, 2008) (10-month delay); *United States v. Gorrell*, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (10-month delay for off-site forensic analysis). The fourth amendment does not subject data searches to any rigid time limit because they may involve much more information than an ordinary document search and require more preparation and a greater degree of care in their execution. 2019 IL App (3d) 170830, ¶ 19 (citing *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 66 (D. Conn. 2002)). Nevertheless, the fourth amendment requires the government to complete its review of digital data “ ‘within a “reasonable” period of time.’ ” *Id.* (quoting *Metter*, 860 F. Supp. 2d at 215). A search of digital data that takes several years may be reasonable as long as the search ends before trial and does not exceed the scope of the original search warrant. See *United States v. Johnston*, 789 F.3d 934, 942-43 (9th Cir. 2015).

¶ 108 We agree with defendant that the acquittal eliminated the probable cause to search for evidence of the sexual assault. But to the extent that defendant argues the eight-month delay in conducting the search was unreasonable, he does not claim that probable cause to search for unauthorized video recording dissipated while the sexual assault prosecution was pending, nor could he, because his data remained secured and unaltered in the EnCase file. He also does not claim prejudice by the delay or that the police department acted in bad faith. See *Burns*, 2008 WL 4542990, at \*9 (search upheld despite “lengthy” delay because the defendant did not assert that “the time lapse affected the probable cause to search the computer (nor could he, given that suspected child pornography had already been found on the hard drive), that the government has acted in bad faith, or that he has been prejudiced in any way by the delay”); see also *Syphers*, 426 F.3d at 469 (the fourth amendment “ ‘contains no requirements about when the search or seizure is to occur

or the duration’ ” (quoting *United States v. Gerber*, 994 F.2d 1556, 1559-60 (11th Cir. 1993)), but “ ‘unreasonable delay in the execution of a warrant that results in the lapse of probable cause will invalidate a warrant’ ” (quoting *United States v. Marin-Buitrago*, 734 F.2d 889, 894 (2d Cir. 1984)). The passage of eight months from the warrant issuance to Feehan’s search was reasonable under the circumstances, considering the intervening sexual assault prosecution, which required the police department to delay its internal investigation, and the sheer volume of data in the EnCase file.

¶ 109

#### H. Plain View

¶ 110

*Hughes* contrasted its facts with

“a circumstance in which the officer was reasonably reviewing data for evidence of drug trafficking and happened to view data implicating defendant in other criminal activity. If such were the case and the data’s ‘incriminating character [was] immediately apparent,’ the plain-view exception would likely apply and permit the state to use the evidence of criminal activity not alleged in the warrant at a subsequent criminal prosecution.” *Hughes*, 958 N.W.2d at 122.

The court’s hypothetical matches this case.

¶ 111

Evidence of a crime may be seized without a warrant under the plain view exception to the warrant requirement. A police officer may properly seize evidence of a crime without a warrant if (1) the officer was lawfully in a position from which to view the object seized in plain view, (2) the object’s incriminating character was immediately apparent, meaning the officer had probable cause to believe the object was contraband or evidence of a crime, and (3) the officer had a lawful right of access to the object itself. *Horton v. California*, 496 U.S. 128, 134-36 (1990). However, “the ‘plain view’ doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.” *Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971).

¶ 112

This case presents the most common use of the plain view doctrine in the context of digital data, which occurs when law enforcement examines a computer pursuant to a search warrant and discovers evidence of a separate crime that falls

outside the scope of the search warrant. The inquiry focuses on whether an officer is exploring hard drive locations and opening files responsive to the warrant, considering both the types of files accessed and the crimes specified in the warrant. *Johnston*, 789 F.3d at 941-43. For example, in *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003), an agent uncovered child pornography on a hard drive while conducting a valid search of the drive for evidence of a murder. Because the agent was properly searching graphics files for evidence of the murder, the child pornography was properly seized and subsequently admitted under the plain view doctrine. *Id.*

¶ 113 We agree with the State that the child pornography was admissible under the plain view doctrine, despite the warrant seeking evidence related to unauthorized video recording. The July 24, 2013, warrant authorized Feehan to search the EnCase file for evidence of the unauthorized video recording, including “any and all digital images, including, but not limited to JPG, GIF, TIF, AVI, MOV, and MPEG files.” Feehan testified that the child pornography was in the JPG file format. The trial court found there was no testimony that the first two images of child pornography were of a different file type or in different areas or directories of the computer than those previously subject to search under the warrant. Defendant does not quarrel with the court’s finding, which is not against the manifest weight of the evidence.

¶ 114 Defendant does not allege that Feehan accessed an area of the hard drive that fell outside the scope of the warrant or that Feehan would have reason to know, before opening the digital images, that they would not contain evidence of the crimes listed on the warrant. Feehan had lawful access to the EnCase file to search for images and video of unauthorized video recording, and he testified that the incriminating character of the two JPG files containing the child pornography was immediately apparent, meaning he had probable cause to believe the files were evidence of a crime. See *Horton*, 496 U.S. at 134. Finding the first two images caused Feehan to suspend his search before securing another warrant to search for additional images of child pornography.

¶ 115 As Feehan’s search was within the scope of the July 24, 2013, warrant and the images of child pornography were admissible under the plain view doctrine, we need not address the State’s alternate argument that the child pornography was

admissible under the good-faith exception to the warrant requirement.

¶ 116

### III. CONCLUSION

¶ 117

To summarize, the warrant authorizing the search of defendant's computer data diminished his expectation of privacy in the types of files described in the warrant. However, any postacquittal search of the same data, directed toward uncovering further evidence of the sexual assault, would have exceeded the scope of the warrant. In this case, Feehan's data search was within the scope of the warrant because it was reasonably directed at uncovering evidence of unauthorized video recording, which was alleged in the warrant. Feehan's search was not directed at finding evidence of criminal activity not described in the warrant. Therefore, the search was reasonable under the fourth amendment and resulted in the lawful discovery of child pornography in plain view.

¶ 118

For the preceding reasons, we hold that the appellate court erred in reversing the trial court's denial of defendant's motion to suppress evidence. We reverse the judgment of the appellate court and affirm the trial court's denial of defendant's motion to suppress the digital images supporting his convictions of child pornography.

¶ 119

Appellate court judgment reversed.

¶ 120

Circuit court judgment affirmed.

¶ 121

JUSTICE NEVILLE, dissenting:

¶ 122

In this case, the majority holds that the police did not violate McCavitt's privacy rights after his acquittal for criminal sexual assault when they searched a copy of the data on his computer hard drive on March 24, 2014, with a search warrant issued on July 24, 2013, because (1) McCavitt's acquittal of criminal sexual assault (a) only partially restored his right to privacy in his computer data involving charges of criminal sexual assault but (b) his acquittal did not restore his privacy rights in evidence of the second offense listed in the July 24, 2013, search warrant—an unauthorized video recording—and (2) police conducted the March 24, 2014,

search within a “reasonable time” after the circuit court issued the July 24, 2013, search warrant.

¶ 123 I agree with the majority that McCavitt had a reasonable expectation of privacy in the data on his computer hard drive. *Supra* ¶ 69. I also agree with the majority that McCavitt’s March 19, 2014, acquittal affected his privacy rights in his property. *Supra* ¶ 70. I disagree with the majority that (1) the search warrant issued on July 24, 2013, remained valid for 243 days until March 24, 2014, for searches for evidence of crimes for which McCavitt was not acquitted that were listed in the July 24, 2013, search warrant and (2) the police could lawfully remain in possession of McCavitt’s hard drive data for 243 days (from July 24, 2013, until March 24, 2014) before the hard drive was searched for data.

¶ 124 I would find that the State’s March 24, 2014, search of McCavitt’s data violated his constitutional and statutory rights for three reasons: (1) McCavitt had a constitutional right to privacy in the personal data on his hard drive and his right to privacy cannot be interfered with or intruded upon without a valid warrant issued after a showing of probable cause; (2) section 108-6 of the Code of Criminal Procedure of 1963 (Code) (725 ILCS 5/108-6 (West 2020)) gave the police 96 hours to execute the July 24, 2013, search warrant and search McCavitt’s hard drive for data, and once the 96 hours expired the search warrant was void (*id.*); and (3) once McCavitt was acquitted on March 19, 2014, section 108-11 of the Code mandated that the trial judge enter an order directing the State to return McCavitt’s property (*id.* § 108-11). Accordingly, I respectfully dissent.

¶ 125 BACKGROUND

¶ 126 On July 17, 2013, the circuit court issued its first warrant to search the single-family residence located at 1710 W. West Aire Avenue in Peoria, Illinois, and the Illinois State Police (ISP) executed the warrant and seized McCavitt’s computer and hard drive.

¶ 127 On July 24, 2013, the circuit court issued its second warrant, at 2:05 p.m., to “search and examine in greater detail” (1) a telephone possessing telephone number (309) 657-4\*\*\* and (2) an LG Computer Tower SN No. WMAZA2914641 that were seized on July 17, 2013, for digital images, for stored and deleted data, for

evidence of criminal activity, and for any evidence of aggravated criminal sexual assault, unlawful restraint, or unauthorized video recording.

¶ 128 The parties stipulated that on July 25, 2013, the ISP transported McCavitt's hard drive to Detective Jeff Avery, a member of the Peoria County Sheriff's Department (PCSD) and a forensic examiner on special assignment to the U.S. Attorney's office. Detective Avery testified that he removed the hard drive from McCavitt's computer, copied it, and saved the copy, called an "EnCase file," to the State's computer. Detective Avery did not testify about the exact date he began his search, but he performed an examination of the EnCase file and found images and videos pertaining to a sexual assault.

¶ 129 After Detective Avery's search, a grand jury indicted McCavitt on August 6, 2013, for the first time, on multiple counts of criminal sexual assault and aggravated criminal sexual assault. On March 19, 2014, a jury found McCavitt not guilty on all of the sexual assault charges. Once the not guilty verdict was returned in open court, McCavitt's attorney made an oral motion requesting that the trial court return items confiscated from McCavitt, including some "collector guns." The court instructed McCavitt's attorney to make his request "in the form of a motion."

¶ 130 On March 21, 2014, two days after McCavitt's acquittal, Detective James Feehan, a computer forensic examiner for the Peoria Police Department (PPD), requested a copy of the EnCase file for purposes of an internal affairs investigation of McCavitt regarding allegations of sexual assault and other possible offenses. On March 24, 2014, Detective Feehan received a copy of Detective Avery's EnCase file, searched it for images of sexual assault "as the [July 24, 2013, search] warrant had authorized," and discovered two images of child pornography.

¶ 131 Also on March 24, 2014, five days after McCavitt's acquittal and pursuant to the trial judge's instructions, his attorney filed a written motion for return of confiscated property.

¶ 132 On March 28, 2014, police arrested McCavitt and charged him with unauthorized video recording. On April 1, 2014, 13 days after McCavitt's acquittal, Feehan obtained a third warrant. Once the circuit court issued the third warrant, Feehan resumed his search and located additional images of child pornography. On



April 23, 2014, a grand jury indicted McCavitt on 10 counts of child pornography and aggravated child pornography.

¶ 133 On April 24, 2014, the circuit court entered a written order that (1) directed ISP to return all guns and weapons to McCavitt *instanter* and (2) “generally continued” McCavitt’s motion for return of confiscated property.

¶ 134 On August 15, 2014, McCavitt filed a motion to suppress evidence in the child pornography case. On October 21, 2014, the circuit court denied McCavitt’s motion to suppress evidence. On July 10, 2015, McCavitt was indicted on seven additional counts of child pornography. On July 14, 2015, a jury found McCavitt guilty of 15 of 17 counts of child pornography. On December 1, 2017, the circuit court sentenced McCavitt to five years’ imprisonment. The appellate court, with one justice dissenting, reversed McCavitt’s conviction. 2019 IL App (3d) 170830. We allowed the State’s petition for leave to appeal. Ill. S. Ct. R. 315 (eff. Oct. 1, 2019).

¶ 135 ANALYSIS

¶ 136 A. Standard of Review

¶ 137 This appeal involves a determination of McCavitt’s rights under Illinois’s constitution (Ill. Const. 1970, art. I, § 6) and statutory provisions (725 ILCS 5/108-6, 108-11 (West 2020)). When construing a constitutional provision, this court’s goal is to determine and effectuate the common understanding of the persons who adopted it—the citizens of this state—and to that end, we will consider the natural and popular meaning of the words used as well as the object to be attained or the evil to be remedied. *Walker v. McGuire*, 2015 IL 117138, ¶ 16. Where the language of a constitutional provision is unambiguous, we give it effect without resort to aids for construction (*id.*), meaning that we will not depart from the plain language of a provision by construing it so that any part is rendered meaningless or superfluous; nor will we read into a provision exceptions, limitations, or conditions that do not appear on its face or that conflict with its intent (*People v. Burge*, 2021 IL 125642, ¶ 34 (citing *People v. Perry*, 224 Ill. 2d 312, 323 (2007))). The interpretation and application of constitutional provisions presents a question of law that we review *de novo*. *Gregg v. Rauner*, 2018 IL 122802, ¶ 23 (citing *Hawthorne v. Village of Olympia Fields*, 204 Ill. 2d 243, 254-55 (2003)). We follow the same rules for

statutory interpretation that we use to construe constitutional provisions, and statutory interpretation also presents a question of law that we review *de novo*. *People v. Wise*, 2021 IL 125392, ¶ 23.

¶ 138 The ultimate issue in this case is whether the March 24, 2014, search of the State’s EnCase file with a search warrant issued 243 days earlier, on July 24, 2013, violated McCavitt’s constitutional and statutory rights. The legality of the March 24, 2014, search is a question of law we review *de novo*. *People v. Bonilla*, 2018 IL 122484, ¶ 10 (citing *People v. Caballes*, 221 Ill. 2d 282, 289 (2006)).

¶ 139 B. McCavitt Had a Constitutional Right  
to Privacy in His Data Under Article I, Section 6,  
of the Illinois Constitution

¶ 140 The Illinois Constitution, unlike the federal constitution, specifically codifies a person’s right to privacy in one’s person, house, papers, and possessions against unreasonable searches and seizures. Ill. Const. 1970, art. I, § 6. Privacy rights are so important to Illinois citizens that the delegates to the sixth constitutional convention codified them in Illinois’s constitution. See also *id.* § 1. “This court has observed that the Illinois Constitution goes beyond federal constitutional guarantees by expressly recognizing a zone of personal privacy, and that the protection of that privacy is stated broadly and without restrictions.” *Kunkel v. Walton*, 179 Ill. 2d 519, 537 (1997); see also Ill. Const. 1970, art. I, § 1. Therefore, article I, section 6, of the Illinois Constitution gives McCavitt a right to privacy in the data on his hard drive. Ill. Const. 1970, art. I, § 6.

¶ 141 C. The July 24, 2013, Search Warrant  
Was Void 96 Hours After  
Its Issuance Under Section 108-6 of the Code

¶ 142 The majority maintains that the March 24, 2014, search pursuant to the search warrant issued on July 24, 2013, was reasonable (1) because of “the intervening sexual assault prosecution” and (2) because of “the sheer volume of data in the EnCase file.” *Supra* ¶ 108.

¶ 143 The majority completely ignores the plain language of section 108-6 of the Code (725 ILCS 5/108-6 (West 2020)). See *supra* ¶¶ 105-08. Section 108-6 provides, in pertinent part, as follows: “The warrant shall be executed within 96 hours [(four days)] from the time of issuance. \*\*\* Any warrant not executed within such time shall be void and shall be returned to the court of the judge issuing the same as ‘not executed’.” 725 ILCS 5/108-6 (West 2020).

¶ 144 The plain language of section 108-6 requires warrants to be executed and searches to be conducted within 96 hours, or four days, after the date and time they were issued, or the warrant is void. See *id.* The July 24, 2013, search warrant directed the police who seized possession of McCavitt’s computer on July 17, 2013, to “search and examine in greater detail \*\*\* an LG computer tower.” There is no language in section 108-6 that tolls the running of the 96 hours (1) because of intervening prosecutions, (2) because of the volume of data in a file being searched, or (3) because of an arbitrator’s ruling or the police department’s collective bargaining agreement (*supra* ¶ 25 n.2). See 725 ILCS 5/108-6 (West 2020). There is also no evidence that the police requested that the trial judge extend the time for the police to search the data on McCavitt’s hard drive. Finally, this court may not depart from section 108-6’s plain language by reading into it exceptions, limitations, or conditions the legislature did not express. *Burge*, 2021 IL 125642, ¶ 20.

¶ 145 The United States Supreme Court provides guidance on what happens when a limitation provision in a search warrant statute expires. In *Sgro v. United States*, 287 U.S. 206, 208 (1932), a commissioner under the National Prohibition Act (Prohibition Act) issued a search warrant on July 6, 1926, pursuant to 18 U.S.C. §§ 613-616 (1926) (repealed). Section 11 of the Prohibition Act required that the “ ‘warrant must be executed and returned to the \*\*\* commissioner who issued it within ten days after its date.’ ” *Sgro*, 287 U.S. at 210 (quoting 18 U.S.C. § 621 (1926)). The Prohibition Act also provided that “ ‘after the expiration of [the 10 days] the warrant, unless executed, is void.’ ” *Id.* (quoting 18 U.S.C. § 11 (1926)). The government did not execute the warrant within 10 days of July 6, 1926. On July 27, 1926, the commissioner redated and reissued the warrant, and the government conducted the search. *Id.* at 208-09. The trial court denied the defendant’s motion to suppress evidence seized under the invalid warrant and admitted the evidence over the defendant’s objection. *Id.* at 208. The Second Circuit

Court of Appeals affirmed. *Id.* (citing *Sgro v. United States*, 54 F.2d 1083 (2d Cir. 1932)).

¶ 146 The Supreme Court noted that there was no provision in the statute that authorized the commissioner to extend the life of the warrant or to revive it. Instead, the government was required to obtain a new warrant and to follow all of the procedures under the statute. *Id.* at 211. The Supreme Court held that, because the original warrant was issued on July 6 and was not executed within 10 days, it became void and could not be redated or reissued by the commissioner. *Id.* at 210-11 (citing 18 U.S.C. § 621 (1926)).

¶ 147 On March 24, 2014, 239 days after the search warrant expired on July 28, 2013, Detective Feehan conducted a search of the EnCase file, leading to the discovery of suspected child pornography. Because the July 24, 2013, search warrant expired on July 28, 2013, and therefore was void (see *id.* at 208-09), the search warrant did not confer any rights on the State or Detective Feehan to conduct the March 24, 2014, search of McCavitt's data. The 243-day delay in searching McCavitt's data was unreasonable and violated McCavitt's constitutional and statutory rights. Ill. Const. 1970, art. I, § 6; 725 ILCS 5/108-6 (West 2020).

¶ 148 The July 24, 2013, search warrant expired on July 28, 2013, and was void (see *Sgro*, 287 U.S. at 208-09), and the search the police conducted on March 24, 2014, 239 days after the search warrant expired, violated section 108-6 (see 725 ILCS 5/108-6 (West 2020); see also *Sgro*, 287 U.S. at 212). Moreover, any evidence that Detective Feehan may have discovered in plain view on March 24, 2014, pursuant to the void July 24, 2013, search warrant was the fruit of the illegal search and must be suppressed. See *Wong Sun v. United States*, 371 U.S. 471, 485-88 (1963) (holding that evidence seized during an unlawful search cannot be used as proof against the victim of the search when the unlawful conduct of the police cannot be purged from the primary taint). Therefore, following *Sgro*, I submit that the July 24, 2013, search warrant became void on July 28, 2013, and that, without a new warrant, no search could take place after that date and any evidence seized was the fruit of the illegal search. *Id.*

¶ 149

D. McCavitt Had a Right to Have  
His Hard Drive Returned Under Section 108-11

¶ 150

The majority takes the position that section 108-11 “contemplates a motion and a hearing before an order is entered disposing of seized items.” *Supra* ¶ 82. I submit that the majority is ignoring the plain language of the statute and, therefore, the trial court’s failure to order the return of McCavitt’s property, *instantly*, cannot be justified by McCavitt’s failure to file a written motion. See 725 ILCS 5/108-11 (West 2020).

¶ 151

Section 108-11 of the Code provides: “The court before which the instruments, articles or things are returned shall enter an order providing for their custody pending further proceedings.” 725 ILCS 5/108-11 (West 2020). There is nothing in the plain language of section 108-11 to support the majority’s position that the statute has a written motion or hearing requirement. See *id.* The majority has read conditions into the statute—a requirement for a motion and a hearing—that are not contained in the plain language of the statute. See *id.* The majority violates this court’s well-established rules of statutory construction that the court will not depart from the plain statutory language by reading in exceptions, limitations, or conditions not expressed by the legislature. *People v. Wise*, 2021 IL 125392, ¶ 23. The majority ignored the language in section 108-11 of the Code when it found that McCavitt failed to file a motion or request a hearing for return of his computer and the data on his hard drive. *Supra* ¶ 82.

¶ 152

When the State seizes property pursuant to a valid warrant (the July 24, 2013, search warrant expired on July 28, 2013, and was void), the custody and disposition of the seized property is controlled by section 108-11 of the Code. See *People ex rel. Carey v. Covelli*, 61 Ill. 2d 394 (1975); 725 ILCS 5/108-11 (West 2020). This court has construed section 108-11 to be the applicable statute when a person seeks the return of property seized by the State. See *Covelli*, 61 Ill. 2d 394. In *Covelli*, the plaintiffs sought the return of their deceased father’s property that police seized pursuant to a search warrant to discover the identity of the person who murdered their father. *Id.* at 398. The plaintiffs argued that section 114-12(a) of the Code (Ill. Rev. Stat. 1973, ch. 38, ¶ 114-12) did not provide a remedy for the return of their father’s property because there were no “defendants” in the case, as no one had been charged with the murder. *Covelli*, 61 Ill. 2d at 402. This court rejected the

plaintiffs’ argument and pointed out that the plaintiffs had “failed to consider article 108 of the Code.” *Id.* This court held that section 108-11 of the Code provided protection to the plaintiffs’ interests in their “property and privacy.” *Id.* at 403.

¶ 153 Section 108-11 gave the trial court, upon McCavitt’s March 19, 2014, acquittal with the entry of the not guilty jury verdict, the authority to order the return of McCavitt’s property *instantly* since the statute did not require McCavitt to file a motion or the judge to hold a hearing. 725 ILCS 5/108-11 (West 2020). It should be noted that, after a hearing on McCavitt’s written motion, the trial judge ordered the return of McCavitt’s guns but continued the remainder of the motion. The trial judge abused his discretion by failing to order a return of the EnCase file upon McCavitt’s acquittal and his attorney’s oral motion on March 19, 2014, because, without a motion or hearing requirement, section 108-11 of the Code gave the trial court authority, *sua sponte*, to enter an order directing the State to return McCavitt’s seized property. See *id.*

¶ 154 1. McCavitt’s Right to His Computer Data  
Was Never Lost So It Did Not Need to Be Restored

¶ 155 The majority maintains, without citation of authority, that McCavitt’s acquittal only partially restored his expectation of privacy in his data. *Supra* ¶ 72. The majority takes the position that, after the March 19, 2014, acquittal, the July 24, 2013, search warrant “still authorized a search for evidence of unauthorized video recording[s].” *Supra* ¶ 106. The majority cites the double jeopardy provision in support of its position that upon McCavitt’s acquittal he only “regained a reasonable expectation that the police would not search his computer for evidence of the offenses of which he was acquitted [on March 19, 2014.]” *Supra* ¶ 76.

¶ 156 I disagree. The double jeopardy provision only prevents McCavitt from being tried a second time for the criminal sexual assault offenses for which he was acquitted. See Ill. Const. 1970, art. I, § 10 (“No person shall be \*\*\* twice put in jeopardy for the same offense.”). The double jeopardy provision did not determine whether McCavitt’s article I, section 6, right to privacy in his computer data was fully restored upon his acquittal.

¶ 157 Illinois’s constitution and statutes codify a right to vote, serve on a jury, and hold public office. See Ill. Const. 1970, art. III, § 1; *id.* art. XIII, § 1; 705 ILCS 305/1, 2 (West 2020); see *Hoskins v. Walker*, 57 Ill. 2d 503, 508-09 (1974) (finding the right to be a candidate for office is not absolute and limitations may be imposed by the legislature). Upon conviction of a felony, Illinois’s constitution and statutes provide that a person shall lose the rights to vote, to serve on a jury, and to hold public office. See Ill. Const. 1970, art. III, § 2; *id.* art. XIII, § 1; 705 ILCS 305/2(a)(3) (West 2020). Illinois’s constitution and statutes also provide that certain rights that are lost because of a conviction of a felony are immediately restored upon completion of the sentence. Ill. Const. 1970, art. III, § 2; 730 ILCS 5/5-5-5(a), (b), (c) (West 2020); 705 ILCS 305/2(a)(3) (West 2020) (“Jurors must be: \*\*\* [f]ree from all legal exception”). Illinois statutes also provide that the rights to vote, to serve on a jury, and to hold public office are automatically restored no later than upon the completion of any sentence for a felony conviction. 705 ILCS 305/2(a)(3) (West 2020); 730 ILCS 5/5-5-5(a), (b), (c) (West 2020). A conviction does not result in the loss of any “civil rights” except as provided by section 5-5-5 of the Unified Code of Corrections (730 ILCS 5/5-5-5 (West 2020)) or sections 29-6 and 29-10 of the Election Code (10 ILCS 5/29-6, 29-10 (West 2020)).

¶ 158 It should be noted that neither Illinois’s constitution nor its statutes provide for a loss of the right to privacy at any time. See Ill. Const. 1970; 730 ILCS 5/5-5-5 (West 2020). I submit that the right to privacy in one’s property, like the rights to vote, serve on a jury, and hold public office, can only be lost, if lost at all, upon conviction of a felony. See Ill. Const. 1970, art. III, § 2; *id.* art. XIII, § 1; 705 ILCS 305/2(a)(3) (West 2020).

¶ 159 Here, McCavitt was only charged with criminal offenses for which he was presumed innocent. See *People v. Robinson*, 167 Ill. 2d 53, 74 (1995). Because McCavitt was acquitted and had not been convicted of a felony on March 19, 2014, he never lost his right to his property and was not required by section 108-11 to take any action, including filing a motion, to have the trial judge return his property. 725 ILCS 5/108-11 (West 2020); see also Ill. Const. 1970, art. I, § 6; *id.* art. I, § 13; *id.* art. XIII, § 1; 705 ILCS 305/2(a)(3) (West 2020); 730 ILCS 5/5-5-5(a), (b), (c) (West 2020). Therefore, since McCavitt’s article I, section 6, right to his property was never lost, and since the two images of child pornography were found by Detective Feehan on March 24, 2014, five days after McCavitt’s acquittal, his





that was void because it was issued 243 days before the search was conducted by the police. *Id.* Second, *Hughes* is also inapposite because there was no Michigan statute like section 108-6 of the Code that placed a 96-hour limit on the execution of a search warrant by the police. See *id.* at 106; Mich. Comp. Laws § 780.651 (2014). Third, *Hughes* is inapposite because the defendant in *Hughes* was not acquitted of certain charges delineated in the warrant. *Hughes*, 958 N.W.2d at 104-05. Therefore, because Detective Feehan could not conduct a search for data within the scope of the void July 24, 2013, search warrant, *Hughes* provides no support for the majority's position.

¶ 165

## CONCLUSION

¶ 166

McCavitt had a constitutional right to the control and possession of his data until the issuance of the July 17, 2013, and July 24, 2013, search warrants. *Riley*, 573 U.S. at 386. Upon the issuance of the July 17, 2013, and July 24, 2013, search warrants, McCavitt's right to his property was temporarily suspended but was never lost because he had not been convicted of a felony on March 24, 2014, and the warrants gave the police 96 hours to search the data on his hard drive. In light of the fact that the July 24, 2013, search warrant became void on July 28, 2013, McCavitt's March 19, 2014, acquittal immediately restored his right to the immediate return of the data in the State's EnCase file. The evidence the police discovered after July 28, 2013, was the fruit of an illegal search with a void search warrant and should not have been admitted into evidence against McCavitt. The legislature should amend section 108-11 of the Code and make it clear that, after an acquittal, a citizen's property (1) that is seized pursuant to a valid search warrant and (2) that is not contraband or obscene must be returned *instantly*. Therefore, I respectfully dissent, and I would affirm the appellate court's judgment and remand this case to the circuit court with directions to exclude all evidence that was discovered by the police during the illegal search conducted by the police after July 28, 2013.