Case No. 125550

IN THE
SUPREME COURT OF ILLINOIS

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

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION AND AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS IN SUPPORT OF DEFENDANT-APPELLEE

Rebecca K. Glenberg
ARDC No. 6322106
Roger Baldwin
Foundation of ACLU, Inc.
150 N. Michigan Ave.,
Suite 600
Chicago, IL 60601
(312) 201-9740
rglenberg@aclu-il.org

Counsel for Amici Curiae
(Additional Counsel Listed on Following Page)

E-FILED
3/9/2021 12:34 PM
Carolyn Taft Grosboll
SUPREME COURT CLERK

On the Brief:

Nusrat J. Choudhury
Roger Baldwin
Foundation of ACLU, Inc.
150 N. Michigan Ave., Suite 600
Chicago, IL 60601

Brett Max Kaufman
Nathan Freed Wessler
American Civil Liberties
Union Foundation
125 Broad Street
New York, NY 10004

Jennifer Stisa Granick
American Civil Liberties
Union Foundation
39 Drumm Street
San Francisco, CA 94111

TABLE OF CONTENTS

Page(s)

POINTS AND AUTHORITIES

INTERESTS OF *AMICI CURIAE*[*]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The American Civil Liberties Union of Illinois ("ACLU of Illinois") is the Illinois state affiliate of the national ACLU.

Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other state and federal courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) and as *amicus* in *People v. Hughes*, No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020), *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The ACLU of Illinois has appeared frequently before this Court advocating for the right to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article 1, Section 6 of the Illinois Constitution. *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186; *People v. Morger*, 2019 IL 123643; *People v. Relerford*, 2017 IL 121094; *People v. Minnis*, 2016 IL 119563; *People v. Caballes*, 221 Ill. 2d 282 (2006); *King v. Ryan*, 153 Ill. 2d 449 (1992); *People v. Adams*, 149 Ill. 2d 331 (1992); *People v. Bartley*, 109 Ill. 2d 273 (1985); *People v. Cook*, 81 Ill. 2d 176 (1980).

---

[*] *Amici* wish to thank Eli Hadley and Santana V. Jackson, students in the Technology Law & Policy Clinic at New York University School of Law, for their contributions to this brief.

FACTUAL BACKGROUND

On July 17, 2013, the Illinois State Police (I.S.P.) obtained a warrant authorizing a search of John T. McCavitt's home and seizure of computers found there. Approximately a week later, on July 24, the I.S.P. obtained a second warrant to search the data stored on a cellphone as well as a LG computer tower. A19-20; A29[1] (together, the "July 2013 warrants"). That second warrant authorized a search for any digital images, stored or deleted data, or other evidence of the crimes of aggravated criminal sexual assault, unlawful restraint, and unauthorized video recording/live video transmission. The affidavit in support of that search warrant alleged that these crimes were committed against a specific and named victim in a single incident that took place the early morning of July 17, 2013. A25-26. There were no allegations to support probable cause for any other crime.

A forensic examiner for the Peoria County Sheriff's Department ("Peoria C.S.D."), Jeff Avery, worked with the I.S.P. to conduct a forensic examination of the LG computer tower. The examiner used EnCase forensic software to create "a bit-by-bit image" reflecting all data on McCavitt's hard drive (hereafter the "EnCase copy"). Tr. Mot. Suppress Evid., R17, 23-24. The examiner then performed the forensic exam. R24-25. Subsequently, in August of 2013, the State charged McCavitt with two sexual-assault-related offenses, to which McCavitt pleaded not guilty. Op. of Ill. App. Ct., Third Dist., A2, ¶ 5. The case proceeded to trial and, on March 19, 2014, a jury found McCavitt not guilty of all charges. *Id.* On that same day, McCavitt orally requested the return of his

[1] Citations to "A_" refer to the Appendix to the Brief of Plaintiff-Appellant People of the State of Illinois (hereinafter "Pl. App. Br."), filed 10/13/20. Citations to "R_" refer to the report of proceedings.

personal property, including his computer. The court denied the request, stating that the property would be returned to him when everything "cooled down." *Id.*

On March 20, 2014, just one day after McCavitt's acquittal, the Peoria Police Department ("Peoria P.D.") initiated an "internal" investigation into McCavitt, an officer at the department. A2, ¶ 6; R30. The following day, the Peoria P.D. forensic examiner, James Feehan, requested and received the EnCase copy from Peoria C.S.D. examiner Avery. *Id.* On March 24, Peoria P.D.'s Feehan began a digital forensic analysis of the EnCase copy, without a warrant (the "March 2014 search"), and saw two images of what he believed to be child pornography. A2, ¶ 6. More than a week later, on April 1, the Peoria P.D. sought and obtained a warrant to further search McCavitt's EnCase copy for images of child pornography. A2, ¶ 7; R34. On April 28, the State indicted McCavitt based on images found in his EnCase copy. A2, ¶ 7. McCavitt filed a motion to suppress the child pornography evidence obtained from the EnCase copy, arguing that the Peoria P.D. had no authority to warrantlessly obtain or examine his hard drive data in March 2014. *Id.*, ¶ 8.

At the suppression hearing, Peoria P.D. examiner Feehan testified that—despite being aware of McCavitt's March acquittal—he had requested the EnCase copy of McCavitt's hard drive, believing "in the back of [his] mind that there was [*sic*] other victims that could be identified." R29-30, R32, R38. He also testified that he "knew," at the time, that Peoria P.D.'s internal investigation "would parallel" a criminal investigation, because "[d]epending on the outcome of the internal [investigation], *** it could possibly be criminal, as [wa]s with most cases [the Peoria P.D.] deal[t] with in circumstances like this." R40-41. Peoria P.D.'s Feehan also testified that he sought and

obtained the April 1 search warrant for two reasons: (1) it would be "safe[r]" to get a warrant "specifically for child pornography," as the prior warrant permitted only searches for evidence of criminal sexual assault and (2) following McCavitt's March 28 arrest, the investigation had shifted from a formal internal investigation to a criminal investigation. R35; Pl. App. Br. 6.

The trial court denied McCavitt's motion to suppress, and, in 2016, a jury convicted him of possession of child pornography. R667-69.

On appeal, the Third District Appellate Court of Illinois reversed the trial court's denial of the motion to suppress, holding that Peoria P.D.'s warrantless search of McCavitt's computer hard drive data following his acquittal on previous unrelated charges violated McCavitt's right to privacy under the Fourth Amendment to the United States Constitution. A1-5. The appellate court held that McCavitt had a diminished expectation of privacy in his seized computer files until his trial was complete. But after that, McCavitt could again expect that he had a full right to privacy in those files. A4, ¶ 24. When Feehan searched McCavitt's EnCase copy without a warrant in March 2014, the search violated that full expectation of privacy. *Id.* ¶ 25. The court also rejected the State's invocation of the good-faith exception to the exclusionary rule, finding that Feehan did not act in good faith in concluding that he could perform a warrantless search of the EnCase copy after McCavitt's acquittal. *Id.* ¶ 31.

SUMMARY OF ARGUMENT

First, under both the Fourth Amendment and Article I, Section 6 of the Illinois Constitution, McCavitt maintained constitutional privacy and possessory interests in the copies of the data on his hard drive—and not just the hard drive itself—that were

searched by law enforcement. As a result, any search of that data presumptively requires a valid warrant.

Second, the State is wrong to insist that its warrantless searches of McCavitt's data are excused by the "second look" doctrine. The March 2014 search at issue here was temporally, purposively, and factually distinct from the earlier searches for evidence pursuant to the July 2013 warrants. In any event, the "second look" doctrine has no application in the context of searches pursuant to warrants, but merely applies to searches of physical items seized incident to arrest and inventoried in police stations. And even if the doctrine did apply here, any "second look" was constitutionally unreasonable under the totality of the circumstances.

Third, the March 2014 search at issue here involved a search for evidence of different crimes committed against different victims than the one authorized by two warrants in July 2013, and the authority of those earlier warrants did not reach the State's post-acquittal searches of McCavitt's data.

Fourth, the State's exploitation of its ongoing possession of a copy of McCavitt's data was constitutionally unreasonable for several reasons. While overseizures of data are often permissible in the context of seizures and searches of digital information, those overseizures are explicitly allowed for the limited purpose of enabling law enforcement to conduct a warranted search based on probable cause. To permit law enforcement to exploit such overseizures beyond the scope of a valid warrant risks permitting any search of digital information to expand into the type of "general search" reviled by the Founders. Moreover, the plain view doctrine does not excuse the State's warrantless search here. The doctrine, which developed in cases involving physical limitations that cabined its

reach, is a poor fit for the digital realm. And to permit the State to overseize data for one purpose but claim the benefit of "plain view" months later would be unreasonable. Finally, that the State engaged in its new searches after McCavitt's acquittal of the crimes under investigation, and for which the original warrants issued, is likewise unreasonable.

ARGUMENT

I. McCavitt maintained both privacy and possessory interests in copies of his hard drive.

Today's computer hard drives store huge volumes of digital data. "Mirroring" software (here, EnCase) creates a perfect replica of the data on a hard drive. R17, 22-23, 46. An individual has the same privacy and possessory interests in their electronic data regardless of whether it is stored on the original hard drive or is a copy of that data, and the State's contrary argument is incorrect.

The Fourth Amendment to the United States Constitution and Article 1, Section 6 of the Illinois Constitution prohibit unreasonable searches and seizures. U.S. Const., amend. IV; Ill. Const. 1970, art. 1, § 6. This Court "interprets the search and seizure clause of the Illinois Constitution in 'limited lockstep' with its federal counterpart." *People v. LeFlore*, 2015 IL 116799, ¶ 16 (quoting *People v. Caballes*, 221 Ill. 2d 282, 314 (2006)). "The essential purpose of the fourth amendment is to impose a standard of reasonableness upon the exercise of discretion by law enforcement officers to safeguard the privacy and security of individuals against arbitrary invasions" (quotation marks omitted). *People v. McDonough*, 239 Ill. 2d 260, 266 (2010).

The Fourth Amendment protects one's reasonable expectation of privacy in intangible material as well as tangible items. *See Warden v. Hayden*, 387 U.S. 294, 304

(1967) (Fourth Amendment protects privacy independent from property concepts). For example, the Fourth Amendment prohibits government eavesdropping on private conversations without a valid warrant. *Berger v. New York*, 388 U.S. 41, 51 (1967) (conversations); *Katz v. United States*, 389 U.S. 347, 353 (1967) (same). The Illinois Constitution similarly offers "protect[ion] [to] people, not places." *People v. Smith*, 152 Ill. 2d 229, 244 (1992) (citing *Katz*, 389 U.S. at 351); *see People v. Pitman*, 211 Ill. 2d 502, 514 (2004).

The constitutional privacy interest in intangibles applies to copies like the EnCase copy. In *Riley v. California*, the Supreme Court permitted police to seize a cell phone without a warrant pursuant to the search-incident-to-arrest doctrine, but barred them from searching the information contained in the phone without further justification. 573 U.S. 373, 403 (2014). In so holding, the Court recognized that the defendant's privacy and possessory interests in the data stored in a phone were separate from—and more extensive than—his interests in the physical phone itself. *Id.* at 393. Moreover, the fact that the police had physical possession of the phone did not diminish the defendant's expectation of privacy in the information stored on the device. Accordingly, the Fourth Amendment's protection "extends not just to the paper on which the information is written or the disc on which it is recorded but also to the information on the paper or disc itself." *United States v. Jefferson*, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008) (holding that taking high-resolution photographs of documents and taking notes on the contents of documents constituted a search and seizure of the information contained in those documents).

Likewise, in this case, McCavitt's privacy interests in the *information* that was stored in his computer at the time it was seized exists separately from his interests in the physical hard drive itself. That the State duplicated that information in the form of the EnCase copy does not change or diminish those interests. *See, e.g.*, Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 703 (2010) (explaining that an individual's "possessory interest extends to both the original and any copies made from it" and that the owner's possessory interest is in "the data"); *see also infra* Part IV.A (explaining the limited purpose of "administrative overseizure" in connection with the seizure and search of information on digital devices).

In the digital age, the Fourth Amendment's protection of privacy and possessory interests in intangible information is more important than ever. Computers, like modern cell phones, hold for many Americans "the privacies of life." *Riley*, 573 U.S. at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Searches of computers, including modern cell phones, would typically expose to the government far more than the most exhaustive search of a house: "A [digital device] 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." *Id.* at 396-97.

Because McCavitt retained a possessory interest and expectation of privacy in the EnCase copy of his hard drive, any search of that data presumptively requires a valid warrant. *Arizona v. Gant*, 556 U.S. 332, 344 (2009). As explained below, no such warrant authorized the March 2014 search conducted by the Peoria P.D.

II. The March 2014 search was not a mere "second look" at previously viewed evidence.

The State represents that its March 2014 search of McCavitt's hard drive was simply a harmless "second look" at the same evidence viewed under the first warrant. Pl. App. Br. 12. This is incorrect.

First, the March 2014 search was temporally, purposively, and factually distinct from the earlier searches for evidence pursuant to the July 2013 warrants. The search was conducted by a different law enforcement agency (the Peoria P.D.) than the one that had conducted the original searches (the Peoria C.S.D.). R17-19. Moreover, the search was explicitly conducted for a new investigative purpose. Indeed, Detective Feehan testified that he was conducting the Peoria P.D. search for an "internal affairs investigation" as well as for evidence of crimes not yet discovered. R30, 32. The March 2014 search sought to uncover never-before-seen evidence of offenses commited against different victims, at different times, and not the single victim and single crime covered by the July 2013 warrants. *Compare* R32 *with* A16-18 *and* 25-28. Further, as the appellate court emphasized, A5, ¶¶ 30-31, the March 2014 search took place the day after a months-long investigation had ended in McCavitt's acquittal. Surely, the State's decision to take McCavitt's case to trial and receive a jury verdict indicated that the I.S.P. and the prosecution had exhausted their criminal investigation, and any subsequent searches of the hard drive were, by definition, in support of a new one.[2]

Second, the "second look" doctrine does not extend to searches conducted pursuant to warrants. As the State concedes, Pl. App. Br. 12-13, this doctrine applies to

[2] The Peoria P.D.'s search would have been entirely pointless had it been intended to simply re-execute prior searches, as the State cannot try McCavitt a second time for the same crimes. *See Brown v. Ohio*, 432 U.S. 161, 165 (1977) (Double Jeopardy Clause "protects against a second prosecution for the same offense after acquittal"); *People v. Stefan*, 146 Ill. 2d 324, 333 (1992) (same).

searches of physical items seized incident to arrest and inventoried in police stations. *See, e.g.*, *United States v. Edwards*, 415 U.S. 800 (1974) (reexamination of a defendant's clothes); *United States v. Burnette*, 698 F.2d 1038 (9th Cir. 1983) (reexamination of a purse); *People v. Richards*, 94 Ill. 2d 92 (1983) (reexamination of a necklace). The State cites no case with a fact pattern remotely similar to this one. Rather, it argues that the "second look" doctrine applies "seamless[ly]" to this case because searches incident to arrest and warranted searches both require probable cause. Pl. App. Br. 13. It represents that *Burnette* "expanded" the logic of *Edwards* "to apply beyond its factual context." *Id.* at 13. But *Burnette*, too, involved a search incident to arrest. *See* 698 F.2d at 1049.[3] The "second look" doctrine is irrelevant in the context of warranted searches because the warrant itself and the Fourth Amendment rules around the execution of that warrant govern the legality of the search. *See infra* Part IV.C.

Third, even if the doctrine applies in this context, "second looks" must be confined to evidence "previously seen" by the government, and cannot be extended to "discover[ies of] new evidence." *Richards*, 94 Ill. 2d at 99; *United States v. Jenkins*, 496 F.2d 57, 74 (2d Cir. 1974) (second look invaded no reasonable expectations of privacy when the police officers "simply looked again at what they had already— lawfully— seen"). Here, the evidence McCavitt sought to suppress was never seen by the

---

[3] The State also cites *United States v. Lackner*, 535 F. App'x 175, 180-181 (3d Cir. 2013) (FBI agents could participate in search pursuant to warrant), *Williams v. Commonwealth*, 527 S.E.2d 131, 136 (Va. 2000) (search of property administratively seized from arrestee), *Hilley v. State*, 484 So. 2d 476, 481 (Ala. Crim. App. 1985) (purse lawfully seized incident to arrest and subject to inventory searches), and *State v. Copridge*, 918 P.2d 1247, 1251-52 (Kan. 1996) (search of property conducted while defendant was being booked into jail). None of these cases come close to supporting the State's argument.

government prior to the March 2014 search. It was obtained via a search for information about victims other than the victim named in the July 2013 warrants. Indeed, as explained *infra* Part IV.B, this information was in government hands in March 2014 only because it knowingly *overseized* McCavitt's entire hard drive as a matter of administrative convenience, rather than seizing only the responsive portions of the drive.

Finally, as the Supreme Court explained in *Edwards*, "second looks" are permitted only for "a reasonable time and to a reasonable extent," 415 U.S. at 809. In other words, they are subject to Fourth Amendment reasonableness, as any search must be. As explained below, it was not reasonable for the government to continue to search McCavitt's private information once he was acquitted. As the Appellate Court wrote, "no reasonably trained officer would conclude that he could perform a warrantless search of a mirrored hard drive that he had no right to possess following the termination of the criminal case against defendant." A5, ¶ 31.

III. The March 2014 search of the EnCase copy exceeded the authority granted by the July 2013 warrants because it involved a search for evidence of different crimes committed against different victims.

The Peoria P.D.'s post-acquittal search was not authorized by the July 2013 warrants. Those warrants permitted a different law enforcement agency to search for evidence of three specified crimes against a single named individual allegedly occurring on July 17, 2013. Neither the July 2013 warrants nor the affidavits supporting them pertained to information from other dates or images of other people. Under the Fourth Amendment, all searches must be within the scope of the warrant authorizing them (and justifying their invasion of a person's reasonable expectation of privacy), and warrants

may not authorize fishing expeditions for evidence of offenses for which there is no probable cause.

A warrant establishes the boundaries of a lawful search. The Fourth Amendment's particularity requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the [Fourth Amendment was] intendeds to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *see also Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (emphasizing that warrants must provide a specific description of the evidence sought). The warrant must be specific enough to ensure that the judge, not the officer, fixes the scope of the search. *Illinois v. Gates*, 462 U.S. 213, 240 (1983).

That scope is limited by the probable cause, demonstrated in a warrant affidavit, to believe that searching a particular place will lead to evidence of a particular crime. Critically, this means that warrants authorize the government to invade privacy interests only with respect to information that is responsive to a valid warrant. Searches for evidence of *other* offenses not described in the warrant are unconstitutional because they are warrantless—and warrantless searches are *per se* unreasonable unless they fall into an exception. *See Katz*, 389 U.S. 347. As the Michigan Supreme Court recently explained:

> [A]s with any other search conducted pursuant to a warrant, a search of digital data from a cell phone 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.

People v. Hughes, No. 158652, 2020 WL 8022850, at *13 (Mich. Dec. 28, 2020) (quoting *United States v. Loera*, 923 F.3d 907, 917, 922 (10th Cir. 2019), and citing *Horton v. California*, 496 U.S. 128, 140-41 (1990)); *see also Gurleski v. United States*,

405 F.2d 253, 258 (5th Cir. 1978) ("[T]he search must be one directed in good faith toward the objects specified in the warrant or for other means and instrumentalities by which the crime charged had been committed.").

In recent years, courts have become especially attuned to the need for strict application of the traditional Fourth Amendment guardrails, like the particularity requirement, to search warrants for digital information. The particularity requirement is especially important in the digital context, where there are few practical barriers to law enforcement's expanding the scope of a search, unless magistrates and the government take careful precautions. As the Supreme Court explained in *Riley*, there are "substantial privacy interests *** at stake when digital data is involved." 573 U.S. at 375. These heightened interests require courts to vigilantly protect the proper bounds of digital searches. *See, e.g., United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (discussing the need for "heightened sensitivity to the particularity requirement in the context of digital searches" due to the vast amount of information that digital devices contain); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (discussing the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant"); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (ability of a computer to store "a huge array" of information "makes the particularity requirement that much more important"); *United States v. Carey*, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999) (discussing the court's "belief that the storage capacity of computers requires a special approach" to particularity and the execution of searches of digital media); *Wheeler v. State*, 135 A.3d 282, 307 (Del. 2016) (risk for warrants for digital and electronic devices to become "general warrants" is

substantial, which "necessitates heightened vigilance, at the outset, on the part of judicial officers to guard against unjustified invasions of privacy"); *State v. Castagnola*, 145 Ohio St.3d 1, 2015-Ohio-1565, ¶¶ 77-78, 46 N.E.3d 638, (due to the large amount of information on computers, officers must be clear about what they are "seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the *warrant*") (emphasis added and citing *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001); *People v. Herrera*, 2015 CO 60, ¶ 18 (in executing a search warrant for evidence related to a suspected crime involving a particular victim, it violates the Fourth Amendment for law enforcement officers to open a file labeled with the name of a different possible victim even where the suspected crime was the same); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 565 (2005) (explaining that without careful attention to particularity, "today's diminished protections are likely to shrink even more as technology advances").

Here, the March 2014 search went beyond scope of the July 2013 warrants, which permitted searches for evidence of criminal sexual assault, unlawful restraint, and unauthorized video recording of a single, named victim stemming from a single incident on July 17, 2013. A16, 19, 21, 27.[4] But the Peoria P.D.'s examiner testified that in March 2014, he went back to search McCavitt's EnCase copy to find evidence related to other, unnamed victims, evidence for which the State had not established probable cause supporting a warrant. *See* Pl. App. Br. 24 ("[Peoria P.D.'s] Feehan explained that he 'knew that there were other victims that could be identified' that could lead to future

[4] The second July 2013 warrant mentioned a video of an unidentified person, but did not provide any reason to believe that that video was surreptiously taken or that that person was an additional victim. A27.

criminal charges."); R32 ("[I]n the back of my mind, I knew that there was [*sic*] other victims that could be identified during the formal [internal affairs investigation] that would turn criminal."); R38 (discussing "the possibility of identifying the other victims during our internal investigation, that possibility existed and then could ultimately come back to State's Attorney's Office for review and possible charges"). This search was conducted for purposes of both criminal and internal affairs investigation. It impermissibly included searches for images that were taken on dates other than July 17.

Because a law enforcement agent intentionally searched for evidence of a crime that was not under investigation and not detailed in the affidavits in support of the July 2013 warrants and thus for which there was no probable cause, the search was warrantless and unconstitutional.

IV. The State unreasonably and unconstitutionally exploited its possession of overseized data that it had no justification to retain once McCavitt was acquitted.

The appellate court correctly held that, once McCavitt was acquitted, the State had no valid interest in retaining the EnCase copy. The State contends that because the Illinois State Police obtained a valid warrant as part of its investigation into McCavitt for a specific incident of aggravated criminal sexual assault, it was permitted to search McCavitt's hard drive months later—even after he was acquitted of the crimes the warrant was intended to investigate. But as explained below, the State only possessed the later-discovered evidence because it had been permitted to seize (and copy) McCavitt's entire drive for a purely administrative purpose—to enable it to search for data that *was* covered by (and justified by the probable cause shown in) the July 2013 warrants. Law enforcement cannot facilitate additional invasions of privacy through this kind of bait and

switch, and neither the plain view doctrine nor the fact of the initial overseizure justified the later search.

A. Overseizures of digital information are sometimes permitted for the limited purpose of facilitating warranted searches for responsive information, but courts must not permit the overseizure to enable law enforcement searches without probable cause.

Searches of digital devices often include the intentional overseizure of information, without probable cause, for law enforcement's administrative convenience. Courts must therefore ensure that searches of this overseized data are strictly limited by probable cause, particularity, and the terms of the warrant lest they become unconstitutional general searches.

Given the vast amount of information housed on digital devices, *Riley*, 573 U.S. at 386, the entire contents of a digital storage medium, like a hard drive, will almost never be responsive to a validly drawn warrant. *Comprehensive Drug Testing*, 621 F.3d at 1168-70 (in the digital context, responsive information will almost always be intermingled with nonresponsive information). However, it is generally challenging for law enforcement to conduct searches of a digital device for responsive information at the scene of that device's seizure. To facilitate forensically sound law enforcement searches of digital data, then, modern warrants regularly permit device seizures, knowing that this will result in an *overseizure* of information, placing into the government's possession information that it has no justification to search. The basis for this practice is that it permits law enforcement to locate and secure responsive information covered by the warrant. *See United States v. Ganias*, 824 F.3d 199, 216 (2d Cir. 2016); *see also, e.g.*, *People v. Thompson*, 28 N.Y.S.3d 237, 258 (Sup. Ct. 2016) ("The Defendant's non-

responsive emails were never properly seized by the People. They were provided as an administrative convenience to allow an effective search.").

Such overseizures are a practical solution to a specific problem, but that solution raises the question of how law enforcement handles, preserves, and uses non-responsive information on seized digital devices. If the government is permitted to seize materials beyond the scope of a properly narrow warrant, but then later exploit the overseizure anytime it wishes—as it did in this case—it undermines the particularity requirement so essential to ensuring that searches and seizures are constitutional. As the appellate court in this case put it, "While police lawfully created the EnCase file to forensically examine defendant's hard drive, they were not entitled to retain the entire EnCase file indefinitely." A4, ¶ 25 (citing *United States v. Premises Known as 608 Taylor Ave.*, 584 F.2d 1297, 1302 (3d Cir. 1978)). That is because permission to search for responsive material connected to probable cause *does not* extend to non-responsive data, information in which an individual maintains a full expectation of privacy. *See, e.g.*, *Hughes*, 2020 WL 8022850, at *9 ("The question here is whether the seizure and search of cell-phone data pursuant to a warrant extinguishes that otherwise reasonable expectation of privacy in the entirety of that seized data. We conclude that it does not. Rather, a warrant authorizing the police to seize and search cell-phone data allows officers to examine the seized data only to the extent reasonably consistent with the scope of the warrant."); *see also* A4, ¶ 25 (citing *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988); *United States v. Veloz*, 109 F. Supp. 3d 305, 313 (D. Mass. 2015); *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that Is*

Stored at Premises Controlledby by Facebook, Inc., 21 F. Supp. 3d 1, 10 (D.D.C. 2013); *Thompson*, 28 N.Y.S.3d at 258-59) .

In *Andresen v. Maryland*, the Supreme Court recognized that there are "grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable." 427 U.S. 463, 482 n.11 (1976). These dangers are amplified when a warrant addresses digital information, where a search will implicate not only great volumes of "papers," but an unprecedented diversity of other private information as well. *See Riley*, 573 U.S. at 394 ("[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. [And] a cell phone's capacity allows even just one type of information to convey far more than previously possible."). Critically, the Supreme Court in *Andresen* observed that the "State was correct in returning [papers that were not within the scope of the warrants or were otherwise improperly seized] voluntarily [to the owner]," and that the "trial judge was correct in suppressing others." 427 U.S. at 482 n.11. The Court cautioned that, when faced with searches and seizures of this scope, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Id.*

Indeed, courts have grown increasingly concerned about unreasonable privacy invasions stemming from careless or opportunistic searches of intermingled digital data. For example, in *Comprehensive Drug Testing Inc.*, the Ninth Circuit explained that administrative overseizure creates a serious risk "that every warrant for electronic

information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." 621 F.3d at 1176. Because overseizure is part of the electronic search process, it requires "greater vigilance on the part of judicial officers in striking the right balance" to ensure that overseizures do "not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id.* at 1177; *see also United States v. Wey*, 256 F. Supp. 3d 355, 407 (S.D.N.Y. 2017) (likening a warrantless search of overseized, non-responsive digital information to "the Government seizing some hard-copy notebooks while leaving others it deemed unresponsive behind, and then returning to the premises two years later to seize the left-behind notebooks based on investigative developments but without seeking a new warrant"); *Thompson*, 28 N.Y.S. 3d at 259 (administrative convenience is not "license for the government to retain tens of thousands of a defendant's non-relevant personal communications to review and study at their leisure"). Other courts have followed that lead, suggesting that flexible *ex ante* protocols be set out by magistrates on a case by case basis to prevent law enforcement from unnecessarily viewing non-responsive files during the execution of a search warrant in the digital context. *In re Search Warrant*, 2012 VT 102, 193 Vt. 51, 71 A.3d 1158 (upholding nine restrictions on a search warrant for electronic data); *United States v. Stetkiw*, No. 18-20579, 2019 WL 2866516 (E.D. Mich., July 3, 2019). As the Supreme Court of Oregon, under its state analogue to the Fourth Amendment, recently explained:

> We acknowledge that, for practical reasons, searches of computers are often comprehensive and therefore are likely to uncover information that goes beyond the probable cause basis for the warrant. In light of that fact, to protect the right to privacy and to avoid permitting the digital equivalent of general warrants, we also hold that Article I, section 9, prevents the state from using evidence found in a computer search unless a valid warrant authorized the search for that particular evidence, or it is

admissible under an exception to the warrant requirement. *State v. Mansor*, 421 P.3d 323, 326 (2018).

Like these courts, this Court should reinforce the importance of exacting and scrupulous application of Fourth Amendment principles to searches of digital information. It is quickly becoming the norm for the government to seize extraordinary amounts of digital data in the pursuit of a narrow slice of information. The government is poised, in other words, to create ever larger stockpiles of information to be searched later, if and when it determines a need—as it did in this case. The result would be a return to the very sort of activity that the Fourth Amendment's drafters meant to combat: the government's indiscriminate and warrantless collection of private information. Instead, this Court should hold that it is unreasonable to retain and search information for which there is no probable cause, and which could have been returned and/or deleted from law enforcement databases or other data storage devices.

B. The Court should not apply the plain view exception in this case.

The Court should reject the State's argument that the plain view doctrine somehow permits law enforcement agencies to engage in new searches of overseized data. The plain view exception to the warrant requirement should not be extended to searches of voluminous digital data, but even to the extent the doctrine might sometimes apply, it cannot justify the search at issue here.

1. The plain view exception, developed for physical-world searches where evidence is tangible and discrete, is a poor fit for searches of digital information.

Exceptions to the warrant requirement, such as the plain view doctrine, do not apply automatically upon invocation; rather, they must remain "tether[ed]" to "the

justifications underlying the *** exception." *Gant*, 556 U.S. at 343. The government bears the burden of demonstrating that an exception to the warrant requirement ought to apply in a given context. *United States v. Jeffers*, 342 U.S. 48, 51 (1951). Time and again, the Supreme Court has refused to "unmoor [warrant] exception[s] from [their] justifications *** and transform what was meant to be an exception into a tool with far broader application." *Collins v. Virginia*, 138 S. Ct. 1663, 1667, 1672-73 (2018). [5]

The Supreme Court has been particularly skeptical of the application of analogue-era exceptions to new digital contexts. *See, e.g.*, *Riley*, 573 U.S. at 393; *see also Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018) (explaining that pre-digital Fourth Amendment precedents cannot be mechanically extended to cases involving digital-age searches). In *Riley*, the Court declined to extend the search-incident-to-arrest exception developed in cases involving arrestees' possession of items like cigarette packs to the digital information contained on an arrestee's cell phone. There, the government "assert[ed] that a search of all data stored on a cell phone [was] 'materially indistinguishable' from searches of *** physical items," but the Court issued a harsh rejoinder:

[5] For example, in *Gant*, the Court declined to extend the search-incident-to-arrest exception to the warrantless search of a passenger compartment in defendant-arrestee's vehicle where it was "unnecessary to protect law enforcement safety and evidentiary interests." 556 U.S. at 346. In *Collins v. Virginia*, the Court held that the automobile exception does not allow an officer to enter a home or its curtilage without a warrant because, unlike vehicles, the curtilage of a home is not readily mobile. 138 S. Ct. at 1672-73. And in *City of Los Angeles v. Patel*, the Court declined to apply the exception for closely regulated industries to warrantless searches of hotel guest registries because, unlike inherently dangerous industries with a history of government oversight such that no proprietor could have a reasonable expectation of privacy, "nothing inherent in the operation of hotels poses a clear and significant risk to the public welfare." 576 U.S. 409, 424 (2015).

> That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom. 573 U.S. at 393.

Holding otherwise would have "untether[ed] the rule from the justifications underlying the [search-incident-to-arrest] exception"—that is, officer safety and evidence preservation. *Id.* at 386.

For similar reasons, the Fourth and Ninth Circuits have recently rejected the government's argument that the "border search exception," which is justified by the government's interest in interdicting physical contraband, could be expanded to permit invasive, suspicionless searches of travelers' electronic devices conducted at a national border. *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019); *United States v. Kolsuz*, 890 F.3d 133, 138 (4th Cir. 2018).

As with these limited exceptions to the warrant requirement, the underlying justifications for the plain view doctrine do not translate to the digital context. In the physical world, the benefits to law enforcement from the plain view exception are limited by the physical characteristics of the things and places for which there is probable cause to search. For example, warrants may easily restrict a physical search to those places large enough to hold the items particularly described in the warrant. Even where police are lawfully in a home, they cannot benefit from plain view by opening a spice box when searching for a rifle. *See, e.g.*, *Horton*, 496 U.S. at 141. Nor can they do so by rummaging through a medicine cabinet while looking for a flat-screen television. *See, e.g.*, *Galpin*,

720 F.3d at 447. However, this common-sense limit is much more difficult to apply in the digital realm, where responsive and non-responsive information is intermingled in computer storage.

Applying the plain view doctrine to searches of digital information presents serious and significant risks that law enforcement will be able to expand what should be limited, probable-cause based incursions into privacy into more generalized, unconstitutional searches. This Court should reject application of the plain view doctrine here.

2. Reliance on the plain view doctrine to exploit an administrative overseizure is unreasonable in this case.

Even if the plain view exception were applicable to searches of digital data, it would not justify the government's search here. First, the plain view exception permits seizure of evidence only when an officer, during the course of a lawful search, comes "inadvertently across a piece of evidence incriminating the accused." *Horton*, 496 U.S. at 135. Officers did not come across the evidence sought to be suppressed in the course of their lawful search pursuant to the July 2013 warrants. Rather, they found the evidence during a subsequent search entirely outside the scope of those warrants. "[A]n essential predicate of the plain view doctrine is that the initial intrusion [does] not violate the Fourth Amendment," *Galpin*, 720 F.3d at 451(quotation marks omitted)—and, as explained *supra* Part III, the March 2014 search exceeded the scope of the July 2013 warrants. *See Hughes*, 2020 WL 8022850, at *17 n.25 (finding that the plain view exception did not apply to a cell phone search that "violate[d] the Fourth Amendment because it was not reasonably directed at uncovering evidence of the criminal activities alleged in the warrant"); *see also United States v. Gurczynski*, 76 M.J. 381, 388

(C.A.A.F. 2017) ("A prerequisite for the application of the plain view doctrine is that the law enforcement officers must have been conducting a lawful search when they stumbled upon evidence in plain view. As noted, the officers in this case were not [doing so] because the execution of the warrant was constitutionally unreasonable.").

Second, it would violate Fourth Amendment reasonableness to allow the State to invoke plain view to take advantage of an administrative courtesy—its initial overseizure, allowed for the specific and limited purpose of permitting a reasonable search for information responsive to the July 2013 warrants—by later searching for and discovering new evidence it had never seen before his acquittal. *See, e.g.*, *Thompson*, 28 N.Y.S. 3d 237; *Wey*, 256 F. Supp. 3d at 407. If this had not been a digital-search case, the government would never have possessed non-responsive material in the first place, let alone retained it up to and beyond his acquittal. But because the data in this case was digital in nature, the State could seize nonresponsive information, then exploit it after Mr. McCavitt's acquittal to develop evidence of new criminal activity that it had never before seen or suspected to exist. Should the State prevail here, law enforcement will make this a regular practice. That is not the purpose of the plain-view exception to the warrant requirement.

C. It was unreasonable for the State to re-search McCavitt's data for evidence after his acquittal without obtaining a new warrant.

Finally, the State's failure to segregate responsive from non-responsive data on his hard drive, at least by the time its prosecution of McCavitt ended, was unreasonable under the Fourth Amendment. When the government seizes entire hard drives to facilitate particularized searches, the Fourth Amendment demands that it identify responsive data in a reasonable way, and within a reasonable amount of time. Here, examining the

"totality of the circumstances" and balancing McCavitt's privacy interest in the non-responsive information on his hard drive against the State's interest in searching that information without a new warrant, the Peoria P.D.'s March 2014 search violated the Fourth Amendment. *Samson v. California*, 547 U.S. 843, 848 (2006); *see Riley*, 573 U.S. at 385-86.

As explained above, McCavitt retained a strong privacy interest in the data on his hard drive even after the State seized and mirrored it. *See supra* Part I; *see also Hughes*, 2020 WL 8022850, at *9; *contra* Pl. App. Br. 24 (relying on the "significantly reduced privacy and possessory interests in any copies of McCavitt's hard drive"). And his privacy interest in data not described in the July 2013 warrants was *never* diminished before the Peoria P.D. searched it in March 2014.

On the other hand, the State's interest in searching the drive without first obtaining a new warrant was miniscule—it could only seek evidence of the crime for which there was probable cause justifying the July 2013 warrants. And as to McCavitt's *non-responsive* data—from which the evidence in this case was drawn—the State had no legitimate interest beyond administrative convenience to hold that data, and could only search it by demonstrating probable cause and obtaining a new warrant that authorized it to do so. *See supra* Part IV.A.

The question of whether the State lawfully *possessed* McCavitt's hard drive even after his acquittal is beside the point. *See* Pl. App. Br. at 27-32. The proper question is not whether the State was legally required to give McCavitt his hard drive back (or delete its copies), but whether it was required, at the very least, to establish probable cause to justify its new invasion of McCavitt's privacy and property interests and obtain a warrant

to exploit anew its possession of his private information. By the time of McCavitt's acquittal in March 2014, the State had effectuated its July 2013 warrants. It had searched the hard drive for responsive data, reviewed, identified, and processed evidence of the potential criminal activity discussed in those warrants, and fully and fairly litigated its charges to a jury verdict.

Once the jury acquitted, whatever authority the State possessed under the July 2013 warrants—namely investigation and possible prosecution of McCavitt for the specific criminal conduct within their scope—had expired. And the State's interest in diving back into the hard drive, without first obtaining a new warrant to authorize further searches, was especially small because—lawfully or not—it continued to possess the hard drive, entirely eliminating any risk of destruction or deletion.

The State attempts to focus the reasonableness analysis on its "interest in investigating" McCavitt based on its "susp[icion" that McCavitt had "committ[ed] criminal conduct in addition to the conduct that resulted in the charges for which he was acquitted." Pl. App. Br. 24. It also asserts that the State had a "pressing need to preserve access to defendant's computer data by retaining a copy" because of the possibility of spoliation. Pl. App. Br. 25. But to investigate new criminal conduct, the State's duty was simple: "get a warrant." *Riley*, 573 U.S. at 403; *see supra* Part III.

CONCLUSION

The Peoria P.D. violated the Fourth Amendment when it searched the copy of his hard drive without after his acquittal without probable cause and a valid warrant. Any evidence derived from that search should be suppressed. The judgment of the Court of Appeals should be affirmed.

Dated: March 3, 2021

Respectfully Submitted,

/s/ *Rebecca K. Glenberg*
Rebecca K. Glenberg
ARDC No. 6322106
Roger Baldwin Foundation of ACLU, Inc.
150 N. Michigan Ave., Suite 600
Chicago, IL 60601
(312) 201-9740
rglenberg@aclu-il.org
Counsel for Amici Curiae

On the Brief:

Nusrat J. Choudhury
Roger Baldwin Foundation of ACLU, Inc.
150 N. Michigan Ave., Suite 600
Chicago, IL 60601

Brett Max Kaufman
Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 345 and 341(a) and (b). The length of this brief, excluding the pages contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, and the certificate of service, is 26 pages.

/s/ *Rebecca K. Glenberg*
Rebecca K. Glenberg
Counsel for Amici Curiae

NOTICE OF FILING AND PROOF OF SERVICE

The undersigned, an attorney, certifies that on March 3, 2021, she caused the foregoing **Motion for Leave** and **Brief of *Amici Curiae* American Civil Liberties Union and American Civil Liberties Union of Illinois in Support of Defendant-Appellee** to be filed with the Clerk of the Supreme Court of Illinois using the Court's electronic filing system and that the same was served by e-mail to the following counsel of record:

Leah M. Bendik
Assistant Attorney General
100 West Randolph Street, 12th Floor
Chicago, Illinois 60601-3218
(312) 814-5029
eserve.criminalappeals@atg.state.il.us

Counsel for Plaintiff-Appellant

Joshua B. Kutnick
900 W Jackson Blvd., Suite 5W
Chicago, IL 60607
joshua@kutnicklaw.com

Counsel for Defendant-Appellee

Within five days of acceptance by the Court, the undersigned also states that she will cause thirteen copies of the **Brief of *Amici Curiae*** to be mailed with postage prepaid to the following address:

Clerk of the Supreme Court of Illinois
Supreme Court Building
200 E. Capitol Ave
Springfield, IL 62701

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct.

/s/ *Rebecca K. Glenberg*
Rebecca K. Glenberg
Counsel for Amici Curiae

E-FILED
3/9/2021 12:34 PM
Carolyn Taft Grosboll
SUPREME COURT CLERK