No. _____

_____

IN THE

SUPREME COURT OF THE UNITED STATES

_____

ASHLEY FERNANDES,
PETITIONER

vs.

COMMONWEALTH OF MASSACHUSETTS,
RESPONDENT

_____

ON PETITION FOR A WRIT OF CERTIORARI

TO THE SUPREME COURT

Leslie W. O'Brien
Post Office Box 31
Pinehurst, MA 01866
781-756-0111
B.B.O. #542413
leslieobrien@comcast.net

Counsel of Record
for the Petitioner

QUESTION PRESENTED

May a search warrant authorize an unlimited search of all of a suspect's digital devices based on an affidavit describing the type of crime being investigated but omitting any cause to believe that evidence of the crime may be found on the devices?

LIST OF PARTIES

The parties below are listed in the caption.

TABLE OF CONTENTS

INDEX TO APPENDICES

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

OPINIONS BELOW

The decision of the Massachusetts Supreme Judicial Court affirming the conviction appears at Appendix A to the petition and is published as *Commonwealth v. Fernandes*, 485 Mass. 172, 148 N.E.3d 361 (2020).

STATEMENT OF JURISDICTION

The date of the opinion and judgment of the First Circuit Court of Appeals of which review is sought is July 6, 2020. This petition is filed within 150 days of that date. The jurisdiction of this Court is invoked under 28 U.S.C. §1257.

CONSTITUTIONAL PROVISION INVOLVED

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

STATEMENT OF THE CASE

To date, the Massachusetts Supreme Judicial Court stands alone among the state courts in holding that a search warrant authorizing an unlimited search of a suspect's digital devices is valid if the type of crime under investigation is described in the warrant even if there has been no showing, and no effort to show, that the devices may contain evidence of the described crime.

The history of this case is as follows:

On May 23, 2008, Ashley Fernandes was indicted for the April 5, 2008, murder of his live-in girlfriend, Jessica Herrera. On the same date, he was indicted for assault and battery and assault with intent to murder Ms. Herrera in December of 2007.

On the day of Fernandes's arrest, during a consent search of his home, police discovered the body of Ms. Herrera. Following the arrest, they applied for a warrant to search the home. The detective who applied for the warrant sought authorization for the seizure of the body of Jessica Herrera as well as physical evidence. Also sought and authorized by the warrant was a search for and seizure of "DVD/VCR tapes, recording devices, cameras and cellular phones (with chargers)." No reason was suggested in the application for the warrant or in the

warrant itself to suspect that this last group of items might contain evidence relevant to the death of Ms. Herrera.[1]

During the search of Fernandes's home, police seized a digital camera, two cell phones, and a computer. While the search was ongoing, a detective found a digital camera in a drawer and gave it to Trooper James Crump. Crump took the camera, turned on the power and hit "playback." The first photograph that appeared on the camera showed Jessica Herrera lying dead on the floor of the home's living room. The trooper then pressed the "back" button on the camera several times and saw additional photographs showing Ms. Herrera's upper body. Two of the photographs show the defendant's hand at Ms. Herrera's neck.

After this discovery, on the next day, Trooper Brian D. O'Neill sought a second search warrant, which authorized the forensic examination - without restriction - of Fernandes's two cell phones, camera, and computer. Plainly recognizing that the application for the first warrant failed to establish probable cause for the search of the camera that had already taken place, Trooper O'Neill added the claim to this second application that it was "not unusual" for killers to photograph their victim's deaths. He did not mention that the camera had already been searched.

---

[1] It has been assumed throughout the litigation in this case that the applications for the search warrants, including the affidavits of the officers, were incorporated into the warrants. See, e.g., *Commonwealth v. Fernandes*, 485 Mass. 172, 184, 148 N.E. 3d 361, 373 (2020).

The vast extent of the permissions requested and granted by magistrate in the second warrant are important to this petition and so are reproduced here.

Following his claim that it is that it was “not unusual” for killers to photograph their victim’s deaths, Trooper O’Neill stated the following in the application for the second warrant:

> “22. ... During the initial search and the subsequent search of the search warrant [sic] executing officers observed a digital camera and a home computer. The discovery of the digital camera at that location indicates the need for the use of a computer with which to manage, download and manipulate images, said computer presumably being the only one located on the premises at 7 Oak St., Peabody, Apt. #9. In consultation with Sergeant Thomas Neff of the Essex County Computer Facilitated Crime Unit (CFCU), [Footnote 1: Sergeant Neff is a twenty-nine year veteran of the Massachusetts State Police and is currently assigned the Essex County District Attorney's Office Computer Facilitated Crime Unit. He has extensive experience in computer crime investigation and the forensic examination of digital data.] I also know that computers, digital cameras and other digital data are used by many to record things and events typically (before the advent of digital technology) relegated to paper; that is, digital data generally - and computers in particular - are, in a sense, electronic filing cabinets. In short, much of a person's personal and professional information is found on the home computer. Sgt. Neff further advises that the convenience afforded by the use of a digital camera, in addition to the anonymity provided to the user of a digital camera, [Footnote 2: In the age of digital still and movie cameras. the elimination of the need for third party film developers (as in the past), has afforded users the ability to photograph illegal images with no fear of exposure] creates a greater likelihood that perpetrators will record such information particularly given the ease with which they believe such images can be destroyed or deleted. [Footnote 3: Images deleted by a user from a digital camera or from a computer are often easily recovered by a forensic examination. The data is not typically physically removed; rather, after deletion, computers and other digital devices merely relegate such files to ‘free space’ merely making that

space eligible for overwriting by new files.] I believe there is probable cause to believe that the materials set forth below (which may exist in tangible form, paper form or in electronic medium on any computer disk and/or computer system) which relate to or have a connection to any item listed below in Items (A) and (B), including but not limited to any document, notes, statements, records, files, correspondence, bill, invoice, forms, logs, books, reports, will be found at the home of Ashley Fernandes located at 7 Oak Street apartment 9 Peabody, Ma. I request permission to search for and SEIZE the following at 7 Oak Street apartment 9 Peabody, Ma: computers, digital cameras, cell phones, digital storage devices and media (disks, tapes, thumb drives) and any and all software and hardware related to computers and other digital devices.

"22. In the case of the digital data--more specifically, two cellular phones, a digital camera and a computer--I respectfully request permission to submit the same to the Essex County CFCU for a forensic examination by Sgt. Neff, Trooper Michael Murphy, or Mr. Richard Falanga, all of whom have extensive training and experience in the forensic examination of all such digital evidence. Said forensic examination will be to search for the above outlined data (graphic evidence of the crime under investigation) and any information linking the defendant to the victim, either through digital photography, digital documentation, e-mail, Internet and chat activity, cellular phone history and cellular phone text messaging. [Footnote 4: Friends and acquaintances in the 'digital age' communicate frequently using the Internet, or using 'chat' rooms or chat software, which allows for dynamic, spontaneous conversation between users. Often, transcripts or partial transcripts of these chats are archived on or remain on the computer, depending on the chat software used and the preferences set by usen of that software.]"

The reference in paragraph 21 to "Items (A) and (B)" is to the following:

"[a.] (1) All objects capable of storing digital data in any form, including but not limited to central processing units ("CPUs"), optical scanners, digital cameras, modems, routers, memory sticks, thumb or USB drivers, firewalls, tapes, zip drive disks, digital video dis.ks ("DVDs"), and computerized printers (which objects, as a whole, shall be

referred to herein as the 'Computer System').

(2) All of the Computer System's documentation, including but not limited to:

(a) Operating System and Application programming disks, software, hardware, CD-ROMs, etcetera;

(b) Manuals, books, or brochures pertaining to computer programs and/or applications;

(c) Manuals, books, or brochures pertaining to an Internet Service Provider(s).

(3) Computer access codes, passwords _and/or protocols.

(4) All evidence of ownership of, access to, and/or control over the Computer System.

b. And to transport the Computer System to a secure location and, there, to EXAMINE said Computer System for the following evidence:

(1) All of the Computer System's documentation, including but not limited *to:*

(a) Operating System and Application programming disks, software, hardware, CD-ROMs, etcetera; 0

(b) Manuals, books, or brochures pertaining to computer computer/programs and/or applications;

(c) Manuals, books, or brochures pertaining to an Internet Service Provider(s).

(2) Computer access codes, passwords and/or protocols.

(3) All evidence of ownership of, access to, and/or control over the Computer System."

On December 15, 2008, the defendant filed his first motion to suppress evidence. The motion asked the court to suppress, among other items, the evidence found as the result of searches of Fernandes's electronic devices since "there was no probable cause to believe that evidence of the crime of homicide would be found stored on any of the electronic devices the police seized and searched."

On February 22, 2011, the motion judge issued his memorandum and decision denying both this first motion to suppress and a second motion filed by

successor counsel.[2] The motion judge noted the deference due to the magistrate's determination of probable cause and cited Trooper O'Neill's claim that he and other experienced officers knew it to be "not unusual" for the deaths of homicide victim's to be memorialized by audio or video means. The judge added a rationale for the search of Fernandes's digital devices that was not included in either of the applications for the warrants. The rationale was that

> "[i]n today's age, computers, cameras, and cell phones often contain reflections of one's relationships with other persons. That is especially so with respect to family members and romantic partners."

Fernandes stood trial in September of 2012. The only evidence the prosecutor introduced at trial resulting from the seizure and search of Fernandes's digital devices was the photographs discovered in the digital camera during the first warranted search.

The prosecutor used the photographs to counter the defendant's claim that the homicide was manslaughter based on reasonable provocation. The prosecutor argued in her opening statement and in summation that the photographs demonstrated that Fernandes took pleasure in killing Ms. Herrera. Fernandes was convicted of first-degree murder on the theories of premeditation and extreme atrocity as well as assault and battery.

---

[2]Later, represented by new counsel, the defendant filed a second motion to suppress the fruits of the search based in part on the failure of the assistant clerk magistrate who examined the warrants, applications, and affidavits to sign the warrant. A.162-63.

On appeal to the Massachusetts Supreme Judicial Court, Fernandes argued that nothing in the first warrant permitted the seizure and search of his camera and nothing in the second warrant remedied the lack of probable cause for the search. The court affirmed Fernandes's convictions on July 6, 2020. *Commonwealth v. Fernandes*, 485 Mass. 172, 148 N.E.3d 361 (2020). Regarding the search of the camera, the court disregarded the trooper's claim in support of the second warrant that it is "not unusual" for killers to photograph their crimes. *Id*. at 184 n.9, 148 N.E.3d at 373 n.9. However, the court found that, because the "type of crime" (the homicide of a domestic partner) was described in the applications for the warrants, it could be "reasonably inferred" by the magistrate that the camera found in the home Fernandes and Herrera shared "would contain evidence relevant to the nature of their relationship, the defendant's motive for the killing, and possibly the killing itself." *Id*. at 183-185, 148 N.E.3d at 373-374.

The Massachusetts court did not comment on the fact that the application for the second warrant did not suggest this second rationale for the search of the camera. Nor did the court elaborate on how one might memorialize the negative aspects of a domestic relationship in photographs.

Fernandes's motion for reconsideration or modification[3] of the decision was denied on July 27, 2020.

REASONS FOR GRANTING THE WRIT

I. The Massachusetts court's holding that a search warrant may authorize an unlimited search of all of a suspect's digital devices based on an affidavit describing the type of crime being investigated but omitting any cause to believe that evidence of the crime may be found on the devices has broad implications.

The Massachusetts court's decision holds that, to establish probable cause to search an accused's digital devices seized during a search of his home, the affidavit in support of the warrant need only allege violence between domestic partners or family members living in the home. *Id.* Although the decision addresses specifically the photographs found in a digital camera, its reasoning applies equally to all the digital devices the warrant authorized police to search.

As stated, the Massachusetts court reasoned that it was inferable from the warrant application that photographs found in a digital camera could be relevant because they may "explain[] the nature of the relationship between the defendant and the victim." *Id*. at 184, 148 N.E. 3d at184. By this same reasoning - simply by virtue of having listed them in the warrant applications - the police in this case

[3] Fernandes asked for modification because the Massachusetts court stated in its decision that Fernandes argued at oral argument that first warrant was sufficient to authorize the seizure of the cameral but additional authorization was required for the search. *Id*. at 185-186. 148 N.E.3d at 374. Fernandes has always argued that neither the initial seizure nor the search of the cameral was supported by a showing of probable cause. See oral argument, https://boston.suffolk.edu/sjc/archive.php.

were authorized to seize and examine, without limitation, any "DVD/VCR tapes, recording devices, cameras and cellular phones" (first warrant) and any "computers ... digital storage devices and media (disks, tapes and thumb drives) and any and all software and hardware related to computers and other digital devices" (second warrant) found in the home. All of these items could contain photographs, which would be admissible under the Massachusetts court's ruling. In addition, some would contain email messages, text messages, personal contacts, financial records, and even more private information that could all be lawfully examined on the theory that such information could conceivably shed light on a family relationship.

The implications of the decision are wide-ranging and not limited to crimes involving violence in the home. The decision implicitly reasons that, if police describe in the warrant application the type of crime being investigated, as long as a magistrate could imagine that evidence of such a crime might be found on a suspect's digital devices police need not state in a warrant application what they are looking for in the devices and why they believe such evidence might be found there. Stated plainly, the decision eliminates the need for a showing of probable cause.

II. The highest state courts in at least three states have held that, to satisfy the need for probable cause, an application for a warrant to search a suspect's digital devices must specify, to the degree practicable, what type of evidence relevant to the crime under investigation is being sought.

In *State v. Mansor*, 383 Or. 185, 421 P.3d 323 (2018), Oregon's high court considered whether a warrant authorizing the search of suspect's four computers was valid. The crime under investigation involved the death of the suspect's infant son and the officer applying for the warrant included this fact in his application. *Id*. at 190, 421 P.3d at 327. The officer also included Mansor's statement to police that he had conducted an internet search when he noticed that the child had alarming symptoms. *Id*.

The court considered Mansor's challenge to the warrant under Article I, § 9 of the Oregon Constitution, the wording of which is nearly identical to the Fourth Amendment. *Id*. at 201-206, 421 P.3d at 336. The article states, in part, that "no warrant shall issue but on probable cause, supported by oath or affirmation, particularly describing the place to be searched, and the persons or things to be seized." *Id*.

The Oregon court concluded that the application for the warrant supported a search of Mansor's computers limited to the internet search he admitted conducting on the date of the child's death. *Id. at* 220, 421 P.3d at 344. However, the state's forensic examiner had conducted an extensive examination of the computers that

included examination of Mansor's internet activity over a period of years. *Id. at* 192, 421 P.3d at 329. The court held that, because the warrant was valid only as to the search for activity on the date of the child's death, all other evidence discovered as a result of the search should have been suppressed. *Id*. at 219-220, 421 P.3d at 343-344.

As in this case, the State argued that the fact that the nature of the crime under investigation was included in the officer's affidavit provided a basis for the issuing judge to find probable cause for the extensive search. *Id.* at 212-213, 421 P.3d at 340. The court rejected this argument, stating that its precedent was

> "not a blanket endorsement of nonspecific terms in search warrants and provide[s] no support for the state's proposed rule that merely identifying the crime under investigation provides sufficient particularity to search the entire contents of a lawfully seized computer."

Id. at 213-214, 421 P.3d at 340.

The *Mansor* court discussed *Riley v. California*, 573 U.S. 373 (2014), where this Court held that the search incident to arrest exception to the warrant requirement did not justify the search of all data on a cell phone that was lawfully seized at the time of a suspect's arrest. Specifically, the Oregon court noted the Court's discussion in *Riley* regarding the "immense storage capacity" of a cell phone as opposed to the limited information in, for instance, a wallet that might be seized during arrest. *Mansor,* 363 Or. at 201-202, 421 P.3d at 334.

The Oregon court also cited a decision by the Delaware Supreme Court, W*heeler v. State*, 135 A.3d 282 (Del. 2016). There, the court considered the validity of warrants that, like the warrants in this case, "covered [the defendant's] entire digital universe and essentially had no limitations." *Id*. at 284, 287. The Delaware court agreed with Wheeler that these were "general warrants" and therefore violated the Fourth Amendment to the United States Constitution and Article I, § 6 of the Delaware Constitution. *Id*. at 294, 298, 305-305.

In *Wheeler*, officers were purportedly investigating allegations of witness tampering. The conduct that was alleged in the search warrant affidavit to be tampering took place in July of 2013. *Id*. at 287. However, the warrant that issued authorized the seizure and unrestricted search of, among other items, all computers, digital media, cell phones, digital cameras and other digital devices and means of storage. *Id*. at 289. During the search of Wheeler' s computer, an investigator opened an image file that appeared to contain child pornography. *Id.* at 291. Based on this discovery, officers obtained a separate warrant to search the seized devices for child pornography. *Id*.

As stated, the Delaware court held that the initial warrant violated both the Fourth Amendment and Article I, § 6 of the Delaware Constitution in that it was both overbroad and lacking in particularity. *Id*. at 298, 304. The court further held that, although it would be unworkable to prescribe hyper-technical rules for

warrants to search digital devices, applications for such warrants must describe what is being seized and searched for "with as much particularity as the circumstances reasonably allow" to avoid offending the constitutional protections against unreasonable searches and seizures. *Id*. at 305. Because the warrants involved lacked such particularity, the *Wheeler* court reversed the lower court's decision denying Wheeler's motion to suppress evidence. *Id*. at 285, 307.

The rule articulated in *Wheeler* is not unduly burdensome. In this case, for example, the applicants for the warrant might have specified that they wanted to search the digital devices for communications between the defendant and the deceased during a specific period of time. Such a request may have rendered a search for such communications lawful. The search of the camera, however, would still have been unlawful absent some separate justification.

In *State v. Castagnola,* 145 Ohio St.3d 1, 46 N.E.3d 638 (2015), the Ohio Supreme Court considered the legality of a warrant to search the defendant's computers. The application for the warrant specified that the crimes under investigation were "retaliation, criminal trespassing, criminal damaging, and possession of criminal tools." *Id*. at 2, N.E.3d at 643. The application sought authority to search, in addition to other items on Castagnolas's premises, his computers, cell phones, hard drives, and other electronic storage devices. The affidavit in support of the warrant quoted text messages provided by a police

source in which Castagnola bragged about finding information about a prosecutor's home and damaging the prosecutor's property. *Id*. at 2-3, 46 N.E.3d at 643-644.

Following issuance of the warrant, a forensic specialist examined the computers. In doing so, she found evidence of child pornography. *Id.* at 3-4, 46 N.E.3d at 644-645. Police obtained a second warrant to search for more evidence of the same. *Id*. at 4, 46 N.E.3d at 645.

Pertinently to this case, the Ohio court considered whether the application for the first warrant was lacking in particularity in that it failed to specify what evidence police were looking for on the computers and why they thought it might be found there. *Id.* at 19, 46 N.E.3d at 657. The Ohio court found that the warrant placed no limitations on the types of records or documents that police could examine in their search of the computers. *Id*. at 19-20, 46 N.E.3d at 657-658. Specifically, the court found that the fact that the type of crime being investigated in was included the warrant application was insufficient to limit the search, and in fact permitted the examiner to view "every record or document" on the computer in question. *Id*. at 20, 46 N.E.3d at 658. The court therefore held that the warrant failed to comply with the requirements of the Fourth Amendment. *Id*. at 659. The *Castagnola* court recognized that the Fourth Amendment does not require a search warrant to apply restrictive search protocols in relation to computers, but, at the

same time, "does prohibit 'a sweeping comprehensive search of a computer's hard drive.'" *Id*. at 21, 46 N.E.3d at 659, citing and quoting from *United States v. Walser*, 275 F.3d 981, 986 (10th Cir.2001).

III. The Massachusetts court's decision disregards the Fourth Amendment's prohibition against general warrants as well as this Court's decisions reaffirming that prohibition.

This Court has famously stated that the Fourth Amendment's particularity requirement is intended to address a specific evil. "[T]he specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion *per se*, but of a general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). More recently, and pertinently to this case, the Court has said that "the presumptive rule against warrantless searches applies with equal force to searches whose only defect is a lack of particularity in the warrant." *Groh v. Ramirez*, 540 U.S. 551, 559 (2004).

The effect of the Massachusetts high court's decision in this case is to permit general rummaging in a suspect's belongings, such as occurred in this case, based on nothing more than a description of the crime being investigated. The decision should not stand.

CONCLUSION

For the reasons stated, the petition for certiorari should be granted.

Respectfully submitted,

ASHLEY FERNANDES

By his attorney,

/s/Leslie W. O'Brien
Attorney for the Petitioner
Post Office Box 31
Pinehurst, MA 01866
781-756-0111
B.B.O. #542413
leslieobrien@comcast.net