NOTICE: All slip opinions and orders are subject to formal revision and are superseded by the advance sheets and bound volumes of the Official Reports. If you find a typographical error or other formal error, please notify the Reporter of Decisions, Supreme Judicial Court, John Adams Courthouse, 1 Pemberton Square, Suite 2500, Boston, MA, 02108-1750; (617) 557-1030; SJCReporter@sjc.state.ma.us

SJC-11793

COMMONWEALTH vs. DENIS DORELAS.

Suffolk. April 7, 2015. - January 14, 2016.

Present: Gants, C.J., Spina, Cordy, Botsford, Duffly, Lenk, & Hines, JJ.

Constitutional Law, Search and seizure, Probable cause. Search and Seizure, Warrant, Probable cause. Probable Cause. Cellular Telephone.

Indictments found and returned in the Superior Court Department on September 27, 2011.

A pretrial motion to suppress evidence was heard by Patrick F. Brady, J.

An application for leave to prosecute an interlocutory appeal was allowed by Botsford, J., in the Supreme Judicial Court for the county of Suffolk, and the case was reported by her to the Appeals Court. The Supreme Judicial Court granted an application for direct appellate review.

Nancy A. Dolberg, Committee for Public Counsel Services, for the defendant.

John P. Zanini, Assistant District Attorney, for the Commonwealth.

Robert E. McDonnell, John Frank Weaver, Arcangelo S. Cella, Matthew R. Segal, Jessie J. Rossman, & Mason Kortz, for American Civil Liberties Union of Massachusetts, amicus curiae, submitted a brief.

CORDY, J. In this case we consider whether, where there was probable cause for the issuance of a warrant to search an Apple iPhone,[1] the search and seizure of certain photograph files conducted in reliance thereon was reasonable.

The warrant authorized a search of the defendant's iPhone for evidence of communications that would link him and another suspect to a shooting that occurred in the Hyde Park section of Boston. The search tool used to extract data from the iPhone was programmed to extract not only contact lists and text messages (texts), but also photographs. Among the photographs extracted and examined by the police were photographs depicting the defendant holding a gun and dressed in the same color jacket described by witnesses to the shooting.

We conclude that where there was probable cause that evidence of communications relating to and linking the defendant to the crimes under investigation would be found in the electronic files on the iPhone, and because such communications can be conveyed or stored in photographic form, a search of the photograph files was reasonable. Finally, we conclude that the

[1] An iPhone, which is manufactured by Apple Inc., is a type of "smart" cellular telephone (smartphone) that, in addition to making telephone calls, can transmit text messages (texts), perform the functions of both a camera and a video recorder, enable the operation of various applications, and connect to the Internet.

photographs in question were properly seized as evidence linking the defendant to the crimes under investigation.

Background. On July 3, 2011, at approximately 7 P.M., Detective Richard Walker and other Boston police officers responded to reports of a shooting at 74 Pierce Street in Hyde Park. On arrival, the responding officers found Michael Lerouge with gunshot wounds to his back. The police found a black Glock, model 23, .40 caliber firearm in the middle of the roadway between 73 and 74 Pierce Street. Witnesses told the police that Lerouge and another person had shot at one another and that Lerouge had discarded the firearm under a parked motor vehicle, after which it slid further into the road. The police were also informed that the other shooter, described as wearing a green-colored shirt or jacket with writing on it, had run down Pierce Street toward Walter Street, dropping a firearm in the process. Witnesses stated that this man stopped, retrieved the dropped firearm, and then continued to run in the direction of 86 Pierce Street. The defendant was subsequently found on the left side of 86 Pierce Street, wearing a green jacket with emblems and suffering from gunshot wounds to his left leg.

When the police found the defendant, he was with Jamal Boucicault, who was subsequently interviewed at the police station. Boucicault told the police that he was visiting the defendant in an apartment at 86 Pierce Street when the defendant

received a telephone call. The defendant began arguing with the caller and subsequently left the apartment. A short time later, Boucicault heard what sounded like gunshots and went outside to find the defendant on the left side of the house at 86 Pierce Street. The defendant handed Boucicault a gun and asked him to hide it, and he then did so in the apartment at 86 Pierce Street.

The defendant's brother, Bricknell Dorelas, also spoke with the police after the incident. He stated that earlier in the evening he had received a telephone call from the defendant, in which the defendant stated that he "was receiving threatening [tele]phone calls and threatening text messages on his [tele]phone." Bricknell did not know the identity of the person who was threatening the defendant. The police also spoke with a cousin of the defendant, Ohuinel Normil, who said the defendant "had been getting a lot of telephone threats because he owes money to people." Normil did not know the identity of these people.

The owner of 86 Pierce Street told the police that he rented the rear apartment on the second floor of the building to the defendant, and that the defendant was the apartment's sole occupant. Thereafter, the police applied for, received, and

executed a search warrant for the defendant's apartment. Pursuant to that warrant, the police seized a gun and an iPhone.[2]

Based on the information above, Walker believed that the defendant's iPhone contained information linking both the defendant and Lerouge to the crimes of assault and battery by means of a dangerous weapon (firearm) and assault with intent to murder that were under investigation. Accordingly, he applied for a warrant to search the iPhone. In his affidavit, which was attached to his application for the warrant, Walker set out the substance of the investigative interviews and concluded by stating: "Based on the above facts . . . I have probable cause to believe [the defendant's] cell phone contains valuable information that will link the victim/suspect ([the defendant]) and suspect/victim (Lerouge) to the crime." Walker received and executed a warrant to search the defendant's iPhone for the following:

> "Subscriber's name and telephone number, contact list, address book, calendar, date book entries, group list, speed dial list, phone configuration information and settings, incoming and outgoing draft sent, deleted text messages, saved, opened, unopened draft sent and deleted electronic mail messages, mobile instant message chat logs and contact information mobile Internet browser and saved

---

[2] The defendant told the police that the iPhone belonged to him. This statement was subsequently suppressed, but the motion judge concluded that there remained "sufficient information" for the magistrate to conclude that the iPhone belonged to the defendant, as he was the sole occupant of the apartment on Pierce Street in which the iPhone was found.

> and deleted photographs on an Apple iPhone, silver and black, green soft rubber case. Additionally, information from the networks and carriers such as subscribers information, call history information, call history containing use times and numbers dialed, called, received and missed."[3]

Among other items, the search resulted in the discovery and seizure of photographs of the defendant wearing a green jacket and holding a gun.[4] The date the photographs were taken, stored, or received is not apparent in the record on the motion to suppress, and the defendant does not claim that the photographs were taken, stored, or received at times remote from the shooting.

Procedural history. In September, 2011, the defendant was charged by a Suffolk County grand jury with possession of a firearm without a license, in violation of G. L. c. 269, § 10 (a); possession of ammunition without a firearm

---

[3] The warrant is awkwardly written, conflating at least in part the items to be searched for and the places to be searched. We agree with the dissent that as written the warrant and the warrant application are overly broad. But considered in conjunction with the affidavit incorporated therein, a commonsense reading shows that the warrant authorized a search of various types of files for evidence of communications that would link the defendant and another person to the shooting. This is the reading that the motion judge appears to have given the warrant.

[4] The complete inventory return lists the following taken as a result of the warrant: "Phone Examination Report Properties" (which includes texts), "Phone Examination Report Index," "Phone Contacts," "Phone Incoming Call List," "Phone Outgoing Call List," "Phone Missed Call List," "Images," and "Video."

identification card, in violation of G. L. c. 269, § 10 (h); carrying a loaded firearm, in violation of G. L. c. 269, § 10 (n); and possession of a large capacity feeding device without a license, in violation of G. L. c. 269, § 10 (m).[5]

The defendant filed a number of motions to suppress evidence, only one of which is relevant on appeal. In March, 2013, he filed a motion to suppress the photographs[6] obtained from the search of his iPhone, which was denied after an evidentiary hearing.[7] In his arguments to the motion judge, the defendant conceded that the search warrant affidavit provided probable cause to search the iPhone for text messages and photographs attached to text messages relevant to the shooting under investigation, but that it was unreasonable to search the

---

[5] Although the defendant was initially charged with offenses related to the shooting, the Commonwealth's investigation determined that the defendant acted in self-defense when he allegedly fired a gun. The fact that subsequent investigation by the police indicated that the defendant was acting in self-defense in the shooting is irrelevant to the validity and scope of the search.

[6] The motion also sought to suppress video recordings obtained during the search. The Commonwealth represented that it would not be using any video recordings recovered from the iPhone, and therefore the defendant has not made any arguments relating to those recordings on appeal. We offer no opinion as to whether video recordings were properly within the scope of the search authorized by the warrant.

[7] The only witness to testify at the evidentiary hearing was Joseph Nicholls, a computer forensics examiner called by the defense.

photograph files on his iPhone for such evidence. The motion judge held, in relevant part, that it was appropriate for the police to search the files on the defendant's iPhone that contained his photographs because the affidavit "furnished probable cause to conduct an electronic search of [his] cell phone" and because threats can be communicated by way of photographs and stored in the iPhone's photograph file. The defendant filed a timely notice of appeal. In July, 2013, a single justice of this court allowed the defendant's petition for leave to file an interlocutory appeal and ordered the appeal to be filed in the Appeals Court. In December, 2014, this court granted the defendant's application for direct appellate review.

Discussion. On appeal, the defendant argues that the motion to suppress photographs was wrongly denied, as there was not probable cause to search his iPhone's photograph file for evidence linking him to Lerouge or the shooting.[8]

When considering the sufficiency of a search warrant application, our review "begins and ends with the four corners of the affidavit" (quotation and citations omitted).[9]

---

[8] The defendant also argues on appeal that the warrant lacked particularity as to the items to be seized and the places to be searched. Where these arguments were not made in the trial court, we do not consider them here.

[9] General Laws c. 276, § 2B, requires that all of the information establishing probable cause be in the affidavit.

Commonwealth v. Cavitt, 460 Mass. 617, 626 (2011). "In determining whether an affidavit justifies a finding of probable cause, the affidavit is considered as a whole and in a commonsense and realistic fashion . . . ." Id. The affidavit should not be "parsed, severed, and subjected to hypercritical analysis" (quotation and citation omitted). Commonwealth v. Donahue, 430 Mass. 710, 712 (2000). "All reasonable inferences which may be drawn from the information in the affidavit may also be considered as to whether probable cause has been established." Id. Importantly, "[w]e give considerable deference to a magistrate's determination of probable cause." Commonwealth v. McDermott, 448 Mass. 750, 767, cert. denied, 552 U.S. 910 (2007).

The Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights "both require a magistrate to determine that probable cause exists before issuing a search warrant" (quotation and citation omitted). Cavitt, 460 Mass. at 626. "[P]robable cause requires a substantial basis . . . for concluding that the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues" (quotations and citations omitted). Commonwealth v. Kaupp, 453 Mass. 102, 110 (2009). See McDermott, 448 Mass. at 768 (probable cause to

search residence where "reasonably likely that the items specified in the affidavit could be found there" [quotation and citations omitted]).[10]

In the physical world, police need not particularize a warrant application to search a property beyond providing a specific address, in part because it would be unrealistic to expect them to be equipped, beforehand, to identify which specific room, closet, drawer, or container within a home will contain the objects of their search. Rather, "[a] lawful search of fixed premises generally extends to the entire area in which the object of the search may be found" (emphasis added). See United States v. Ross, 456 U.S. 798, 820 (1982).

However, in the virtual world, it is not enough to simply permit a search to extend anywhere the targeted electronic objects possibly could be found, as data possibly could be found anywhere within an electronic device. Thus, what might have

[10] General Laws c. 276, § 1, provides that a court or justice is authorized to issue a warrant "if satisfied that there is probable cause" for the complainant's sworn belief "that any of the property or articles hereinafter named are concealed in a house, place, vessel or vehicle." The warrant must also identify the property and name or describe "the person or place to be searched." Id.

been an appropriate limitation in the physical world becomes a limitation without consequence in the virtual one.[11]

Nevertheless, much like a home, such devices can still appropriately be searched when there is probable cause to believe they contain particularized evidence. See McDermott, 448 Mass. at 770-772. However, given the properties that render an iPhone distinct from the closed containers regularly seen in the physical world, a search of its many files must be done with special care and satisfy a more narrow and demanding standard. See Hawkins v. State, 290 Ga. 785, 786-787 (2012) (cellular telephone is "roughly analogous" to container, but large volume

[11] We recognize that individuals have significant privacy interests at stake in their iPhones and that the probable cause requirement of search warrants under both the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights serves to protect these interests. In its recent landmark decision of Riley v. California, 134 S. Ct. 2473, 2488-2491 (2014), the United States Supreme Court explained how the privacy interests implicated in smartphone searches "dwarf" those in cases in which a limited information is contained in a finite space, given the volume, variety, and sensitivity of the information either stored in a smartphone or stored remotely and accessed through a smartphone. Calling a smartphone a "phone" is a "misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." Id. at 2489. "They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." Id. See Commonwealth v. Phifer, 463 Mass. 790, 797 (2012). An iPhone has the same operating system as an Apple computer. In 2014, the storage capacities of iPhones ranged from sixteen to sixty-four gigabytes. See Riley, supra at 2489. Such devices can hold hundreds of thousands of files, including millions of pages of text and thousands of photographs. See id.

of information contained in cellular telephone "has substantial import as to the scope of the permitted search," which must be done with "great care and caution"). "Officers must be clear as to what it is they are seeking on the [iPhone] and conduct the search in a way that avoids searching files of types not identified in the warrant." United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001), cert. denied, 535 U.S. 1069 (2002). "[A] computer search 'may be as extensive as reasonably required to locate the items described in the warrant'" based on probable cause (emphasis added). United States v. Grimmett, 439 F.3d 1263, 1270 (10th Cir. 2006), quoting United States v. Wuagneux, 683 F.2d 1343, 1352 (11th Cir. 1982), cert. denied, 464 U.S. 814 (1983).

In the instant case, the police presented evidence in the warrant affidavit that included the statements of witnesses to the effect that the defendant had been receiving threatening communications on his iPhone with respect to money he owed to "people," and indeed had been using his iPhone while arguing with an individual immediately prior to the shooting. This was admittedly sufficient to establish probable cause to believe that the defendant's iPhone likely contained evidence of multiple contentious communications between himself and other persons in the days leading up to the shooting, that is, evidence of communications both received as well as initiated

and sent by the defendant that would link him and others to that shooting. The warrant, in turn, included authorization to search for such evidence not only in the iPhone's call history and text message files, but also in its photograph files.

The defendant contends, however, that the police had probable cause only to search his telephone call and text files, and not his photograph file. We disagree. Communications can come in many forms including photographic, which the defendant freely admits. So long as such evidence may reasonably be found in the file containing the defendant's photographs, that file may be searched.[12,13] We agree with the motion judge that the

---

[12] Photographs received or sent as attachments to texts may be stored in the iPhone's photograph file as well as in the text file. In addition, the iPhone can take photographs of texts, which then are stored in the photograph file.

[13] Although some of our case law discussing searches of physical containers has employed language of "reasonableness," see, e.g., Commonwealth v. Signorine, 404 Mass. 400, 405 (1989) ("It is clear that a valid search may include any area, place, or container reasonably capable of containing the object of the search"), in practice, most fixed premises cases still analyze whether the physical container at issue was "capable of containing the object of the search" (emphasis added). Id., quoting United States v. Percival, 756 F.2d 600, 612 (7th Cir. 1985). See Commonwealth v. Wills, 398 Mass. 768, 774 (1986) (photograph album "could have concealed a small knife" [emphasis added]). Given the differences between searches of physical and virtual places, at a minimum, the standard that governs the proper scope of a search of an electronic device, such as the iPhone here, for evidence for which probable cause has been found is whether that evidence might reasonably be found in the electronic files searched; "capable of containing" is far too broad.

evidence sought, for which there was probable cause, might reasonably have been found in the photograph file. Therefore, a search for such evidence in that file was neither outside the scope of the warrant nor unreasonable.

Nevertheless, the defendant contends that a search using the Universal Forensic Extraction Device (UFED) could easily have been conducted for communications, including photographic communications, without reviewing his photograph file.[14] As explained by the defense expert at the evidentiary hearing, the UFED is capable of performing targeted searches of this type, distinguishing between areas of the iPhone from which to extract data -- such as "call logs," "phonebooks," "[short message service],"[15] "pictures," and "videos" -- and retrieving photographs that may have been attached to text messages.

While it may be possible for a forensic examiner to retrieve some photographic evidence through searches of files other than the photograph file, that does not make such a

---

[14] The Universal Forensic Extraction Device (UFED) connects to a cellular telephone by a cable and has a port for insertion of a memory drive, on which extracted information can be stored. When connected and turned on, the UFED offers the examiner a choice of extraction methods.

[15] In selecting short message service as the type of data to extract using the UFED, the police would have access to the content of both simple texts and "multimedia message service" texts with photographs or other items attached, regardless of whether they had been saved or deleted.

retrieval method constitutionally required where such photographic evidence would also reasonably be found in the iPhone's photograph file. In addition, the communications at issue may have occurred over an extended period of time leading up to the shooting, and where texts and their attachments may be overwritten by new data, the saved photographic attachment may only be found in the iPhone's photograph file. Accordingly, in determining the nexus between the items sought and the place to be searched, it was reasonable here to infer that the targeted evidence might not exist exclusively in the text and call log folders. See Commonwealth v. O'Day, 440 Mass. 296, 302 (2003) (magistrate may make probable cause determination in part based on "normal inferences as to where a criminal would be likely to hide [evidence of the crime]" [citation omitted]). The affidavit in question contained enough information from which the magistrate and the forensic examiners could conclude that the evidence sought might reasonably be located in the photograph file. See McDermott, 448 Mass. at 767.

The dissent postulates that even if the warrant did authorize the search and seizure of photographs, such authorization extended, at most, to photographs depicting threats. Post at . However, there is no conceivable way for the police to detect whether a picture is of a threatening nature without opening it first. See United States v. Burgess,

576 F.3d 1078, 1094 (10th Cir.), cert. denied, 558 U.S. 1097 (2009). Once the photographs in question were viewed, their evidentiary relevance linking the defendant (holding a gun and wearing a jacket similar to the one worn by the shooter) to the specific crimes under investigation was apparent. The photographs also came within the scope and subject matter of the warrant, as one or more of them could well have been sent as a threatening communication to the person or persons who had apparently been threatening him over several days.[16]

The motion to suppress was properly denied.[17]

So ordered.

[16] We need not resort to the plain view doctrine in this case, and we recognize that the application of that doctrine to digital file searches may, at times, need to be limited, see Preventive Med. Assocs. v. Commonwealth, 465 Mass. 810, 831-832 (2013); United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010).

[17] While the scope of the search in this instance might have been unreasonable if the photographs had been discovered as the result of reviewing photographs received, taken, or stored long before the events leading up to the shooting, there is no argument that that occurred here.

LENK, J. (dissenting, with whom Duffly and Hines, JJ., join). The architects of art. 14 of the Massachusetts Declaration of Rights and the Fourth Amendment to the United States Constitution had in mind only searches of physical places and seizures of physical objects. Transposing these protections to digital contexts is an ongoing and challenging task, as the matter before us only underscores. I disagree with the court's resolution of the issues presented here. In my view, the search of the photograph files on the defendant's Apple iPhone "smart" cellular telephone was not supported by probable cause, and the warrant authorizing that search was not sufficiently particular. Furthermore, even had there been probable cause to support a search of the photograph files, the photographs seized by the police appear to have been outside the permissible scope of the warrant. I write separately for these reasons, and also to express my concern about the future direction of our search and seizure law in a digital context.

In an increasingly digital world, we continue to lean heavily on analogies between digital media and physical spaces and objects, such as that between a computer and a closed container. See, e.g., Commonwealth v. McDermott, 448 Mass. 750, 771-772, cert. denied, 552 U.S. 910 (2007) (McDermott). In reality, however, searches of physical spaces for physical

objects are akin to searches of digital media for digital information much in the way that "a ride on horseback" resembles "a flight to the moon." Riley v. California, 134 S. Ct. 2473, 2488 (2014) (Riley). As a result, if we are to preserve the values that art. 14 and the Fourth Amendment seek to protect, we must view more critically our reliance on physical analogs, which may hamper rather than enhance our analyses; we also must be amenable to considering new paradigms that may advance our thinking. See generally Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476 (2011).

1. Probable cause. Probable cause requires "a 'substantial basis' . . . for concluding that 'the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched'" (citation omitted). Commonwealth v. Kaupp, 453 Mass. 102, 110 (2009) (Kaupp). The digital media at issue in this case,[1] however, do not fit neatly within this framework.

[1] The photographs that the defendant seeks to suppress were seized as the result of a three-part process. First, soon after the shooting in which the defendant was wounded, police searched his apartment pursuant to a warrant and seized his iPhone, among other items. Next, pursuant to a separate warrant, a Boston police department forensic examiner used a targeted data extraction technique to copy certain categories of files from the iPhone. Finally, the extracted files were studied to

What was the "place" to be searched -- the defendant's iPhone as a whole? Or only certain parts of it? And what were the "items" to be seized -- categories of files? Or were they certain files, perhaps specific photographs of evidentiary value? See Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 551-557 (2005) (Kerr, Digital World) (discussing meaning of digital "search"). See generally Kerr, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, Tex. Tech L. Rev. (forthcoming) (on pages 23-28 of manuscript, discussing meaning of digital "seizure").

As the court acknowledges, the warrant at issue here does not provide easy answers to these questions. Ante at note 3. The property that the warrant authorized the police to search for and seize consisted principally of enumerated categories of files, including "saved and deleted photographs."[2] The warrant

---

determine whether they contained the information sought. The search and seizure at issue here encompass the second and third of these stages, as the first stage was conducted pursuant to a separate warrant, not now contested.

[2] Each photograph on the iPhone is stored in a separate file. The other categories of files listed in the warrant were the iPhone's "contact list, address book, calendar, date book entries, group list, speed dial list, phone configuration

stated that these files were located "on an Apple iPhone" described by its physical appearance, which itself was situated at the Boston police department building in the Hyde Park section of Boston. Yet the warrant also incorporated by reference an affidavit that appeared to envision a broader, content-based search of the device. The affidavit concluded that probable cause existed to believe the defendant's iPhone contained "valuable information" linking the defendant and his interlocutor to the crime.

Given this lack of clarity, the court correctly determines that the warrant for the iPhone describes the place to be searched as the physical device itself, and the items to be seized as the categories of files that it lists. See ante at note 3. The court incorrectly holds, however, that there was probable cause to search the entire set of photograph files on the defendant's iPhone. In my view, there was not a substantial basis for concluding that the entire set of the defendant's photograph files, rather than just the subset of photograph

---

information and settings, incoming and outgoing draft[,] sent, [and] deleted text messages, saved, opened, unopened[,] draft[,] sent[,] and deleted electronic mail messages, mobile instant message chat logs and contact information[, and] mobile internet browser."

files attached to the defendant's text and multimedia messages, was related to the criminal activity under investigation.[3]

An affidavit in support of a search warrant must be read "in an ordinary, commonsense manner, without hypertechnical analysis." See Commonwealth v. Cruz, 430 Mass. 838, 840 (2000), and cases cited. This principle applies even where a search ventures into the vast store of private information available on a device like an iPhone. The probable cause analysis is limited to "the facts recited in the affidavit and any reasonable inferences therefrom." Kaupp, supra at 107, citing Commonwealth v. Allen, 406 Mass. 575, 578 (1990).

Read in an ordinary, commonsense manner, and without resorting to hypertechnical analysis, the facts in the affidavit and the reasonable inferences to be drawn from them did not provide probable cause to search the entire set of the defendant's photograph files. In addition to recounting other facts concerning the shooting, the affidavit reported, based on the statements of three individuals, that the defendant had been receiving threatening telephone calls and text messages, and

---

[3] Review of the denial of a motion to suppress is appropriate where, as here, "the ultimate findings and rulings bear on issues of constitutional dimension." Commonwealth v. McDermott, 448 Mass. 750, 762 (2007), quoting Commonwealth v. Haas, 373 Mass. 545, 550 (1977), S.C., 398 Mass. 806 (1986).

that he had been arguing on the telephone shortly before the shooting. This information provided probable cause to believe only that the iPhone's files pertaining to calls and text messages would offer evidence of communications linking the defendant to the shooting. The iPhone's lists of incoming, outgoing, and missed calls could have shed light on the identities of the individuals threatening the defendant and arguing with him. Its text message files could have provided similar information, and also could have revealed the content of some threats made against the defendant. According to the forensic expert, extraction of the text message files also would have retrieved any photographs attached to those messages, see ante at **note 15**, and the defendant has no quarrel with that fact.

What the affidavit did not provide was reason to believe that the iPhone's entire set of photograph files, as opposed to only those photograph files attached to calls or text messages, would present evidence related to the shooting. In the abstract, I do not disagree with the court's statement that "[c]ommunications can come in many forms including photographic." Ante at . Nor, apparently, does the defendant. A photograph depicting a severed horse's head, for

instance, might well be used to communicate a threat (in the mode of "The Godfather" novel and motion picture). But the hypothetical viability of communication by photographic suggestion, even had it been mentioned in the affidavit, would not have supported a reasonable, commonsensical inference that a search of the defendant's entire set of photograph files was needed to produce the subset of photographs that might at some point have been communicated.

The court reasons that, if a photograph file attached to a text message had been deleted and overwritten by new data, access to the entire set of photograph files on the iPhone might be necessary for a forensic investigator to find another copy of that specific file on the device. Ante at . As the court notes, however, there is no argument that the photographs at issue here were "received, taken, or stored long before the events leading up to the shooting" -- the situation in which, in the ordinary course, photographs that had been attached to text messages would have been most likely to have been deleted and overwritten by new data.[4] See ante at note 17.

[4] In some circumstances, it might be natural to suspect that data deliberately has been concealed from inquiring eyes. See, e.g., United States v. Gray, 78 F. Supp. 2d 524, 527 n.5 (E.D. Va. 1999) (discussing investigation of hacking offenses). The

In sum, the information presented to the magistrate did not create even a "[s]trong reason to suspect" that the entire set of photograph files on the defendant's iPhone were related to the criminal activity being investigated, much less a "substantial basis" for such a belief (citations omitted). See Kaupp, supra at 110-111, and cases cited. The search of those files was not supported by probable cause, and consequently it was unconstitutional.[5]

While there was surely probable cause to believe that there was evidence of the communications described in the affidavit somewhere within the defendant's iPhone, the essence of the United States Supreme Court's decision in Riley, supra, was that

---

facts set forth in the affidavit circumscribing our analysis, however, did not suggest that data concealment was otherwise a concern in this case. In any event, when an initial search leads a forensic investigator to believe that files have been deleted or otherwise concealed, the investigator of course may seek an additional warrant to perform a more far-reaching search for those files.

[5] The Commonwealth argues that suppression is not warranted even if the search for the defendant's photograph files was improper. "We have not adopted the 'good faith' exception for purposes of art. 14 of the Massachusetts Declaration of Rights or statutory violations, focusing instead on whether the violations are substantial and prejudicial." Commonwealth v. Hernandez, 456 Mass. 528, 533 (2010). But "all violations of . . . probable cause requirements are substantial." Commonwealth v. Sheppard, 394 Mass. 381, 389 (1985). See Commonwealth v. Nelson, 460 Mass. 564, 571 (2011).

such devices cannot be treated like ordinary containers. This is because "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." Riley, supra at 2491. In one commentator's words, "limiting a search to a particular computer is something like . . . limiting a search to the entire city." Kerr, Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279, 303 (2005).

We must not be taken in by the shape and size of a device that permits access to massive stores of information of different kinds. Where possible -- recognizing that it not always is -- it may be best to treat such a device more like a city than like a packing crate. Here, there was no impediment to limiting the search to certain types and categories of files stored in specific sections of the iPhone's data storage. Because there was no substantial basis for believing that the entire set of photograph files on the defendant's iPhone contained evidence related to the shooting, that portion of the iPhone should not have been included in the "place" to be searched.

2. Particularity. Article 14 and the Fourth Amendment also require that a warrant identify with particularity the

place to be searched and the items to be seized. The requisite particularity, however, was not present in this case.[6]

Read commonsensically, the affidavit and warrant both envisioned a general search of the entire iPhone, rather than a targeted search for certain types of communications. Based on the facts it presents, the affidavit draws the general conclusion that the defendant's iPhone "contains valuable information that will link the [defendant] and [another person] to the crime." The affidavit proceeds to explain that, accordingly, permission is being sought to search the iPhone for a wide variety of categories of files. Several of these, such as the defendant's "[s]peed dial list," "[p]hone configuration information and settings," and "[m]obile Internet browser," were most unlikely to contain any evidence of the criminal activity under investigation. The warrant, in turn, authorized the

---

[6] The court declines to consider the defendant's particularity arguments to the extent they were not raised in the Superior Court. See ante at note 8. However, these arguments were fairly raised: the defendant argued specifically that "[t]he particularity requirement serves as a safeguard against general exploratory rummaging by the police through a person's belongings," quoting Commonwealth v. Freiberg, 405 Mass. 282, 298, cert. denied, 493 U.S. 940 (1989). In addition, he contended that "the warrant became an impermissible general search." Contrast Commonwealth v. Garcia, 409 Mass. 675, 678-679 (1991) ("An issue not fairly raised before the trial judge will not be considered for the first time on appeal").

seizure of most of the categories of files on the defendant's iPhone, including all "saved and deleted photographs."[7]

Allowing the police to search a broad variety of categories of files, many of which were at most tangentially related to the communications described in the affidavit, was an "end run" around the particularity requirement. Particularity should mean more than just a general directive to the police to look until they find something.

Creating particularized limitations beforehand for a search of a device capable of storing hundreds of thousands of files is difficult. But it is not impossible. As the court acknowledges, current search technology already allows forensic examiners to pinpoint their searches. Ante at . Accordingly, the warrant could have limited the search only to the iPhone's call records and text message files -- the categories of files most likely to provide evidence of the "threatening phone calls and threatening text messages" that

[7] With regard to the reasonableness of the search's execution, it also may be noted that video recording files were extracted from the iPhone even though those files were not named in the warrant either as places to be searched or as items to be seized. See ante at note 6.

preceded the shooting.[8] The warrant also could have limited the search of any images files temporally to include only images stored on the device in the days or weeks leading up to the shooting. Compare United States v. Winn, 79 F. Supp. 3d 904, 921 (S.D. Ill. 2015) ("Most importantly, the warrant should have specified the relevant time frame"). Restrictions of this sort would prevent forensic investigators from exercising greater discretion than art. 14 and the Fourth Amendment allow. As the United States Supreme Court noted in Riley, supra at 2495, the

[8] Courts in other jurisdictions have taken this approach. See United States v. Winn, 79 F. Supp. 3d 904, 922 (S.D. Ill. 2015) (deeming warrant overbroad that did not limit seizure to "a very small and specific subset of data" or "describe that data with as much particularity as the circumstances allowed"). See also Matter of Black iPhone 4, 27 F. Supp. 3d 74, 79-80 (D.D.C. 2014) (requiring government to provide greater particularity with respect to procedures that would be used to avoid viewing material outside scope of warrant to search iPhone); State v. Henderson, 289 Neb. 271, 289 (2014), cert. denied, 135 S. Ct. 2845 (2015) (concluding that warrant for search of cellular telephone "must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search"). Cf. Preventive Med. Assocs. v. Commonwealth, 465 Mass. 810, 829 (2013) (permitting use of "taint team" to screen out privileged electronic mail messages prior to review by investigator or prosecutor). The United States Court of Appeals for the Tenth Circuit concluded in United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir.), cert. denied, 558 U.S. 1097 (2009), that review after the fact of the reasonableness of a given search satisfied the particularity requirement, but acknowledged that such review "may be problematic" in some contexts. Requiring a particularized warrant beforehand avoids these potential problems.

fact that technology now enables an individual to store huge sums of information in his or her pocket "does not make the information any less worthy of the protection for which the Founders fought."

3. Scope of the search. Finally, the photographs that the defendant seeks to suppress do not seem to have been within the scope of the search that the court deems permissible. Two of the four photographs at issue apparently show the defendant in possession of a gun, and two show him wearing a green jacket. It is possible that these images provided some measure of support for the inference that the defendant had participated in the shooting, since witnesses had seen one of the shooters wearing a green shirt or jacket. See ante at . The photographs were not, however, the kind of evidence that the police were (according to the court) permitted to be searching for -- namely, communications relating to the shooting.

The court accordingly devises the hypothesis that the contested photographs "could well have been sent as a threatening communication to the person or persons who had apparently been threatening [the defendant]." Ante at . This hypothesis is implausible. The court's theory is not rooted in an evaluation of the photographs, given that they are

not part of the record before us. The Commonwealth, having examined the photographs, has not suggested that they constituted, singly or together, a "threatening communication" made by the defendant to anyone. Nor does the available information support such an interpretation.

The affidavit described three interviews concerning the communications for which, on the court's view, the warrant authorized a search. According to the first interview, the defendant "received a [tele]phone call and started arguing with the caller on the [tele]phone," and "left the apartment still arguing with the caller" shortly before the shooting took place. According to the second interview, the defendant "was receiving threatening [tele]phone calls and threatening text messages on his [tele]phone." According to the third interview, the defendant had "been getting a lot of telephone threats because he owe[d] money to people."

These interviews do not support the view that the photographs in question were included in the communications described. The first interview clearly described a telephone call rather than an exchange of picture messages. While the second and third interviews did not rule out the possibility that the threats described were communicated in photographs,

both interviews specified that the threats were received, not sent. Nothing in the affidavit suggests that the defendant was using photographs of himself to threaten others. Moreover, even if the two photographs of the defendant holding a gun were intended as a threat, it strains credulity to assert that photographs of the defendant wearing a green jacket had a similar purpose. In sum, I question whether the forensic investigators reasonably could have understood the photographs at issue to be communications related to the shooting. By extension, the photographs would not be ones that the investigators were, on the court's analysis, permitted to seize.

A corresponding flaw occurring in a physical search could have been cured by the "plain view" doctrine, according to which, "if officers, in the course of conducting a lawful search, discover evidence in plain view, such evidence may be seized." See McDermott, supra at 777, citing United States v. Gray, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999). Yet, recognizing that "the application of that doctrine to digital file searches may, at times, need to be limited," ante at note 16, and sources cited, the court resists wholesale importation of the plain view doctrine into the current context.

There is good reason for the court's caution on this score. Although the search at issue in this case was, according to the court, limited to "evidence of communications that would link the defendant and another person to the shooting," ante at note 3, the plain view doctrine would render that constraint meaningless, given that "there is no conceivable way" to detect whether a picture is relevant evidence without first looking at it. See ante at .

It is an open question whether application of the plain view doctrine to searches of digital media would undermine the constitutional prohibition on general searches.[9] This court applied the plain view doctrine to a search of computer files in McDermott, supra at 777. More recently, however, the court expressed concern that a search of digital files could be "joined with the plain view doctrine to enable the Commonwealth to use against defendants inculpatory evidence . . . even though

[9] See, e.g., United States v. Galpin, 720 F.3d 436, 451 (2d Cir. 2013); United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176-1177 (9th Cir. 2010); Note, Digital Searches and the Fourth Amendment: The Interplay Between the Plain View Doctrine and Search-Protocol Warrant Restrictions, 49 Am. Crim. L. Rev. 301 (2012); Note, Computer Seizures and Searches: Rethinking the Applicability of the Plain View Doctrine, 83 Temple L. Rev. 1097 (2011). See also United States v. Ganias, 755 F.3d 125, 137-140 (2d Cir. 2014), reh'g en banc granted, 791 F.3d 290 (2015) (government not permitted to retain indefinitely nonresponsive documents seized in permissible search).

such evidence may not actually fit within the scope of the search warrants obtained." Preventive Med. Assocs. v. Commonwealth, 465 Mass. 810, 831-832 (2013) (Preventive Med. Assocs.). This prospect is worrisome because searches of digital information tend to require law enforcement to delve into, and carefully sift through, large stores of data. See United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176-1177 (9th Cir. 2010). The result is that "rules created to prevent general searches for physical evidence may result in the equivalent of general searches for digital evidence." Kerr, Digital World, supra at 566.

In Preventive Med. Assocs., supra at 832, this court elected to "leave for another day the question whether use of the plain view doctrine as a justification for admission of evidence should be precluded or at least narrowed in the context of searches for electronic records." While not today, the day when the court will be called upon to determine more precisely when and how the plain view exception applies to digital searches is likely close at hand.