IN THE SUPREME COURT OF THE
STATE OF OREGON

STATE OF OREGON,
Petitioner on Review,
v.
KALIQ MICHAEL MANSOR,
Respondent on Review.
(CC C111376CR) (CA A153124) (SC S064382)

On review from the Court of Appeals.*

Argued and submitted June 15, 2017.

Peenesh Shah, Assistant Attorney General, Salem, argued the cause and filed the briefs for the petitioner on review. Also on the briefs were Ellen F. Rosenblum, Attorney General, and Benjamin Gutman, Solicitor General.

Joshua B. Crowther, Chief Deputy Defender, Office of Public Defense Services, Salem, argued the cause and filed the brief for the respondent on review. Also on the briefs was Ernest G. Lannet, Chief Defender.

Before Balmer, Chief Justice, and Kistler, Walters, Nakamoto, Flynn, Duncan, and Nelson, Justices.**

BALMER, C. J.

The decision of the Court of Appeals is affirmed. The judgment of the circuit court is reversed, and the case is remanded to the circuit court for further proceedings.

---

* Appeal from Washington County Circuit Court, Donald R. Letourneau, Judge. 279 Or App 778, 381 P3d 930 (2016).

** Landau, J., retired December 31, 2017, and did not participate in the decision of this case. Brewer, J., retired June 30, 2017, and did not participate in the decision of this case.

BALMER, C. J.

In this case, we consider defendant's challenge under Article I, section 9, of the Oregon Constitution, to a warrant that authorized the search, seizure, and examination of his computer. Police investigated the injury of defendant's infant son while in defendant's care on June 12, 2011. The infant later died at the hospital. Defendant told the police that his son had struggled to breathe and that he had used his computer to look online for first aid advice before calling 9-1-1. For that and other reasons, police seized and then searched defendant's computer as part of their investigation. The forensic examination of the computer found internet search history shortly before the 9-1-1 call that was generally consistent with defendant's statements, but the examination also revealed that defendant had visited websites and entered search terms related to the abuse of infants several times in the months and weeks prior to the infant's death. The trial court denied defendant's motion to suppress the latter evidence, and defendant was convicted of murder and other crimes. The Court of Appeals reversed the convictions, concluding that the warrant authorizing the search of the computer violated the particularity requirement of Article I, section 9, because it permitted the examination of everything on defendant's computer. *State v. Mansor*, 279 Or App 778, 801, 381 P3d 930 (2016). We allowed the state's petition for review of that decision and now affirm, although our analysis differs in some respects from that of the Court of Appeals.

For the reasons discussed below, we conclude that the application of Article I, section 9, to warranted searches of personal electronic devices requires a test that protects an individual's right to be free from unreasonable searches and seizures while also recognizing the government's lawful authority to obtain evidence in criminal investigations, including through searches of digital data. A warrant to search a computer or other digital device for information related to a crime must be based on probable cause to believe that such information will be found on the device. To satisfy the particularity requirement of Article I, section 9, the warrant must identify, as specifically as reasonably possible in the circumstances, the information to be searched for,

including, if available and relevant, the time period during which the information was created, accessed, or otherwise used. 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.

In this case, police had probable cause to believe that defendant's computer would contain information regarding defendant's internet searches shortly before his 9-1-1 call. We refer to that information as "the June 12 internet search history." Defendant moved to suppress all of the information found through the forensic examination of the computer, which, as noted, included the evidence of child abuse and other crimes dating from weeks and months before the 9-1-1 call, as well as the June 12 internet search history. The trial court found that the police lacked probable cause to search the computer for any information beyond the June 12 internet search history. Nevertheless, the trial court denied defendant's motion to suppress, and virtually all of the relevant forensic evidence was admitted at trial. That was error. In our view, the warrant was sufficiently particular to permit a search of the computer; however, the trial court erred in admitting the proffered evidence that was obtained as a result of the forensic examination, because, as we read the warrant, it authorized the police to search only for the June 12 internet search history. Accordingly, we conclude that defendant's motion to suppress should have been granted in part and denied in part. Because that error was not harmless, we affirm the Court of Appeals' decision reversing defendant's convictions and remand the case to the trial court.

I. FACTS AND PROCEEDINGS BELOW

On June 12, 2011, defendant called 9-1-1 at 2:22 p.m. and reported that his 11-week-old son, B, had stopped

breathing. After an ambulance took the infant to the hospital, Detective Rookhuyzen of the Washington County Sheriff's Office child abuse unit interviewed defendant at his home. On the basis of information learned in that interview and a pediatrician's examination of B at the hospital, Rookhuyzen applied for and obtained the warrant which defendant now challenges.

Rookhuyzen prepared a seven-page affidavit in support of his warrant application. The Court of Appeals summarized the affidavit's contents, which recounted Rookhuyzen's interactions with defendant and observations of the home:

> "At the beginning of the interview, Rookhuyzen noted that defendant was 'non-emotive'—which, in Rookhuyzen's training and experience, was 'highly unusual' in such circumstances because '[p]arents are usually crying, sobbing, and exhibiting signs of sadness or anxiety.' Defendant told Rookhuyzen that he had been home alone with B and his twin brother, while his wife was working. According to defendant, as he had been feeding B a mixture of formula and liquid vitamins, the mixture had started to come out of the baby's nose and the baby had started coughing, so defendant had turned him over, shaken him, and 'smacked' him on the back. The baby's eyes became 'fixed' and 'droopy,' and his breathing became 'very much labored.' Defendant told Rookhuyzen that he then shook B more, and the baby began going 'a minute or two between breaths.'
>
> "Defendant did not call 9-1-1 at that point. Instead, he told Rookhuyzen, he 'went online' on a computer in the baby's room to conduct research about what he should do. When, after 15 minutes, the baby's condition did not improve, defendant called 9-1-1.
>
> "Defendant did not call his wife during that period—and, indeed, had not attempted to contact her by the time Rookhuyzen began to interview him. In Rookhuyzen's experience, that was 'extremely unusual': '[W]ith these kind of incidents, spouses want to call each other instantly, even before speaking with law enforcement.'
>
> "Rookhuyzen's affidavit further recounted that, at the hospital, B was examined by a pediatrician, Dr. Lindsay, who determined that the baby had no brain activity and

would die soon. Lindsay further determined, *inter alia*, that the baby had experienced head trauma resulting in a skull fracture, bi-lateral retinal hemorrhages, and an 'old rib fracture.' In Lindsay's opinion, defendant's account was not consistent with the baby's condition, and he ultimately rendered a diagnosis of 'shaken baby syndrome' as a result of intentionally inflicted abuse.

"*** Further, as specifically pertinent to the lawfulness of the seizure and search of defendant's computers, the affidavit included the following averment:

> "'I know based upon my training and experience that computers can be connected to the internet to find information using computer software that browse internet sites for information. Internet search engine sites such as Google and Yahoo! are often used to search the internet for information related to a user's requests. I know that the computer will retain a history of internet sites visited and the search terms used on the internet. I know that to retain the integrity of a computer's memory and how the system was used, the computer needs to be searched in a laboratory and carefully examined by a trained computer forensic examiner in order to ensure that the data is not corrupted, damaged, or otherwise changed from the time when the machine was seized. [Defendant] told me that he searched the internet between the time he noticed [B] was having difficulty breathing and the time he called emergency dispatch. He told me that he was using a computer to search the internet for advice on what he should do. When I was in the residence, I saw two laptop computers and two desktop computers. [Defendant] did not specify which computer he was using just before he called 9-1-1.'

"The affidavit also included a detailed description of defendant's residence. Finally, in a section titled 'Conclusion,' the affidavit stated Rookhuyzen's belief that there was probable cause to seize and search 11 types of evidence, including '[t]wo laptop computers in the residence' and '[t]wo desktop computer towers located in the office/baby room.'"

Mansor, 279 Or App at 780-81 (brackets in *Mansor*; footnotes omitted).

A circuit court judge signed the search warrant that evening. The search warrant instructed executing

officers to "seize and search and forensically examine the following objects: See attachment A." (Emphasis omitted.) Attachment A was captioned "items to be searched for, to be seized, and to be analyzed." It repeated verbatim the list of eleven items included in Rookhuyzen's affidavit, including "[t]wo laptop computers" and "[t]wo desktop computer towers." The warrant itself contained no instructions or limitations regarding how the computers were to be analyzed.

The warrant was executed that night. Two laptop computers, two desktop computers, and other items from B's room were seized. The computers were taken to the Northwest Regional Computer Forensics Laboratory, operated by the FBI, which performed the forensic analysis. The lab's report summarized the request:

> "[Rookhuyzen] requested that the [seized computer drives] be examined for internet history and internet search terms input by the user on [June 12] especially from 2pm onward. Per a discussion with Det. Rookhuyzen, the suspect searched the internet 15 minutes prior to calling 9-1-1 in regards to his 11-week old child suffering injuries. Suspect claimed that the internet searches were regarding how to aid an injured infant. Pertinent examination results should be regarding child abuse and a possible history thereof."

When Rookhuyzen made the initial request to the lab, he provided a list of 19 search terms. A week later, another detective, Hays, added eight more search terms.[1]

The scope of the analysis of the computers expanded further. The report noted that about a month after the initial request, a detective directed that the search of the computer be expanded to include email, although no relevant emails were ultimately located. The forensic examiners also included in the report search terms that were not provided by the detectives, but that, in their opinion, "yielded possibly pertinent results."[2] The forensic examiner stated that

[1] Initially, Rookhuyzen provided the following search terms: bruise, police, child abuse, investigation, rib, fracture, broken rib, colic [spelled as "cholic"], baby, babies, twin, breath, breathing, rescue, rescue breathing, CPR, care, abuse, and physical abuse. Later, Hays added: father, anger / angry, crying, hurt / hurting, infant, evidence, explaining, and injuries.

[2] Those search terms included "swelling," "Kaliq Mansor," "911," and "Go the Fuck to Sleep."

he had no knowledge of the case itself, other than what he had learned from the detective's request regarding the examination of the computers.

The report also summarized the lab's methods and findings. For each computer and laptop, the storage media were removed and imaged.[3] An initial analysis revealed that some of the hard drives had last been used in 2009, and those were not examined further. For the remaining drives, the forensic examiner assembled a "complete Internet history," including "deleted Internet history records." "Internet history" is a broad term. The software used by the lab—"Net Analysis"—compiled many types of data, for example, cookies, cached data, "leaks," and other types of data that are generated as part of normal internet browsing activity, to create the internet history dataset.[4] Each piece of internet history data might contain or be associated with information useful to investigators, such as the identity of the computer user logged in at the time, the time and date that a particular web page was visited, or search terms entered into search engines, but each piece of data was not associated with all of those types of information. For example, not all records were associated with a date and time or revealed how the user navigated to a particular web page.

The internet history dataset was compiled into a large spreadsheet containing over 360,000 records dating back to 2005—six years before B was born. Net Analysis allowed the forensic examiner to search for text in any of the

[3] At trial, the forensic examiner testified that imaging digital storage media means making "an exact bit-by-bit duplication of all of the data on the hard drive. *** [A]ll examination from that point on is done on [that] image, so that if anything should happen to corrupt the data, I'm not corrupting the original hard drive. *** So it maintains the integrity of the original evidence." *See also* ORS 133.539(1)(a)(A) ("'Forensic imaging' means using an electronic device to download or transfer raw data from a portable electronic device onto another medium of digital storage.").

[4] The forensic examiner also explained many of those terms. A cookie is "a little piece of data that [a] website is going to leave on your local computer that will help you the next time you access the same website." Cached data is information on a web page that a computer stores locally, enabling faster loading the next time the user accesses the same web page. A leak is "an artifact of browsing history. It basically means the browser was trying to delete a piece of the Internet history just for normal cleanup or if the history was trying to be deleted by a user, *** and for some reason it couldn't *** so it sort of generates an error and that error is called a leak."

websites visited and to organize the internet history records by date and time. In addition to a printed summary of its findings, the lab provided detectives with a DVD containing that dataset and several lengthy reports on specific searches requested by detectives. For example, one report listed all web URLs visited on the date of the 9-1-1 call, beginning with a visit to Netflix nine seconds after midnight and continuing until that afternoon. That report is 630 pages long. Another report that listed results for the search term "abuse" was 101 pages long, and contained URLs dating from a 16 month period as well as many other URLs not associated with a date and time. The lab also provided reports for the search terms that "originated during the examination" as yielding "possibly pertinent results," listed above. Similarly, the DVD contained files that were not internet history, but that the forensic examiner believed might be relevant, such as a Microsoft Word document containing a narrative description of the child's birth, photos of B, and a downloaded computer game that allowed the user to simulate child abuse.

Before trial, defendant moved to suppress the evidence discovered on the computers, arguing that the warrant was "worded so broadly as to constitute a general warrant." Defendant suggested that "search protocols" should have been included in the warrant to restrict the potentially unlimited search of the computer hard drives. A search protocol, for example, could limit the search to specific files or types of data on the computer—such as emails, internet searches, or photographs—or to search terms used in an internet browser. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F3d 1162, 1179 (9th Cir 2010) (on rehearing en banc) (Kozinski, C.J., concurring) (discussing search protocols in warrants to search computers).

The trial court denied the motion in a written opinion. The trial court first noted that defendant had conceded that the search warrant properly permitted law enforcement officials to search the computers for the June 12 internet search history. The court then rejected defendant's argument that the lack of search protocols in the warrant rendered the warrant unconstitutional, noting that the majority view is that such protocols are not constitutionally required. The court found that the affidavit did not provide

probable cause to search the computer for evidence of any crimes other than those related to B's injuries on June 12. Nevertheless, and apparently relying on the "traditional rules for the plain view exception," the court concluded that "all evidence obtained through the execution of the warrant [was] admissible."[5]

At trial, Detective Hays relied on the forensic lab's reports to testify about defendant's internet history. He stated that shortly before the 9-1-1 call, defendant searched the term "baby pulse no breathing"—a search consistent with defendant's explanation of events. The focus of Hays's testimony on defendant's internet history, however, was computer activity that occurred before that day. Interpreting reports generated by the forensic examiner, Hays concluded that on five separate occasions—the day of the 9-1-1 call and four earlier occasions, the earliest 54 days before the call—the computer had been used to conduct searches about or related to child abuse. The prosecutor implied that the search terms typed into the computer, often in quick succession, provided a snapshot of defendant's thought process and conduct. For example, three days before the 9-1-1 call, there were many relevant searches, including, at 6:24 a.m., a search for "afraid of abusing my baby," then shortly after that, "how do I deal with a screaming baby," then three minutes later, "baby, swelling, back of head."[6]

The evidence gathered from defendant's computer was undoubtedly helpful to the state's case. In the state's closing argument, the prosecutor called internet search history "a looking glass" into a person's character and "a record

[5] The plain view doctrine "permit[s] the officers to seize evidence without a warrant if, in the course of executing [the] search warrant and while they were in a place where they had a right to be, they had probable cause to believe that evidence that they saw was either contraband or evidence of a crime." *State v. Carter,* 342 Or 39, 45, 147 P3d 1151 (2006). The state did not rely on the "plain view" exception to the warrant requirement in the Court of Appeals and does not rely upon that exception before this court. We discuss the doctrine again briefly later in this opinion.

[6] Detective Hays testified about other incriminating phrases that appeared in the search history without disclosing the date of those searches. Those included "how do I stop abusing my baby," "infant abuse," "signs of newborn abuse," "holding baby upside down cause brain damage," "infant attachment father," "how to quiet a crying infant," "abuser therapy," "battered newborn," and "father hates infant."

of what's going on in [defendant's] head." The prosecutor recited strings of sequential search terms to the jury, such as those quoted above, and used those to speculate about defendant's thought process. Defendant's ex-wife and B's mother also relied on the internet history to understand what had happened. She said that in the first two weeks after B's death, she supported defendant because she couldn't believe that he would hurt B. But "[w]hen the evidence came to light about [defendant's] computer searches, I stopped supporting him."

The state charged defendant with six counts relating to three discrete incidents of abuse against B and B's twin in the weeks before B's death, and four counts relating to the incident that caused B's death. After an eleven day trial, the jury convicted defendant of all charged counts: murder, assault in the first degree, three counts of assault in the third degree, and three counts of criminal mistreatment in the first degree.

On appeal, defendant challenged the warrant as facially invalid because it failed to satisfy the particularity requirement of Article I, section 9, of the Oregon Constitution. Defendant also asserted that, to determine whether the warrant was valid, the court should look at the warrant alone and not consider information contained in the affidavit that supported the warrant application.

The Court of Appeals first addressed whether its review of the warrant was limited to the face of the warrant or whether it also could look at the affidavit. *Mansor*, 279 Or App at 788. It noted that the state had introduced evidence at trial that supported its contention that the affidavit was attached to the warrant at the time defendant's house was searched, and that defendant had not produced any evidence to the contrary. *Id.* at 790. A defendant bears the burden to rebut the presumption that a warranted search is valid. *State v. Walker*, 350 Or 540, 553, 258 P3d 1228 (2011). Because defendant had not presented any evidence supporting his argument, the court held that it would consider the contents of the affidavit in the challenge to the warrant. *Mansor*, 279 Or App at 791.

But on the broader issue of the warrant's validity, the court held that, even considering the information in the affidavit as well as the warrant, the warrant was unconstitutionally overbroad in authorizing the forensic examination of defendant's computers. It recognized that the case presented a question of first impression and reviewed decisions from other courts, some of which invalidated computer search warrants for failing to meet particularity requirements. It quoted with approval *Wheeler v. State*, 135 A3d 282 (Del 2016), which adopted a requirement that warrants "describe what investigating officers believe will be found on electronic devices with as much specificity as possible under the circumstances." *Mansor*, 279 Or App at 796 (quoting *Wheeler*, 135 A3d at 304). The court, in light of the "unique functionality and capacity of electronic devices," concluded that

> "for purposes of the constitutional particularity requirement, personal electronic devices are more akin to the 'place' to be searched than to the 'thing' to be seized and examined. Concomitantly, that requires that the search of that 'place' be limited to the 'thing(s)'—the digital data—for which there is probable cause to search."

Id. at 801.[7]

The court then applied that rule. It read the warrant and affidavit as establishing probable cause

> "with respect to internet searches during the 15-minute period preceding the 9-1-1 call—and, arguably, with respect to all electronic communications and photos during the entire time that B was in defendant's care on June 12, 2011. However, nothing in Rookhuyzen's affidavit established probable cause that a temporally unlimited examination of the contents of defendant's computers, including of files and functions unrelated to internet searches and emails, would yield other evidence of the events of June 12, 2011."

Id. at 802. The court also found that the trial court's error in denying the motion to suppress was not harmless and, for those reasons, reversed and remanded. We allowed the state's petition for review to consider those important issues.

---

[7] The Court of Appeals and the parties used the terms "location" and "place" as a convenient way to discuss searches of electronic devices, but they acknowledge that those analogies are imperfect. We agree and, for reasons discussed in the text, find the analytical value of those analogies to be limited.

II. THE DIGITAL CONTEXT

Before addressing the parties' legal arguments, it is helpful to identify some of the ways that digital data, whether stored on a computer or other digital device, differs from physical evidence. First, raw digital data—the 1s and 0s that make up binary signals—must be processed and displayed by intermediating programs and hardware to be meaningful. A user may conceive of the information on her computer as being "files," organized into "folders" that are stored in various locations on the computer and accessed through particular software programs. But a computer forensic examiner views the same data differently. As demonstrated by the facts of this case, a category of information that is a likely source of evidence—say, the internet search history on a given computer—may be composed of many types of data and files, and the physical locations of data on a computer hard drive and even the software's organization of those data and files may be unrelated to the user's perception of how their data is organized. *See* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 Berkeley J Crim L 112, 128 (2011) (explaining that "files do not correspond to organizational choices made by computer users").

Similarly, some data on a computer may not be in the form of "files." For example, when a user deletes a file, fragments of the file's raw data often continue to exist on the hard drive. A forensic examiner may be able to reconstitute a new file from that residual data that can then be read by a program. That concept—that digital information is perceived in fundamentally different ways by users than by forensic examiners—means that a user's honest statements about a file, such as "it's in the 'My Documents' folder," "that document is gone, I didn't save it," or "no one can use my computer without my password," may not be "true" to a forensic examiner.[8] We discuss the implications of the foregoing context below.

---

[8] Forensic examiners have many potential sources of evidence not apparent to a casual computer user:

> "When a computer user accesses a web site, opens a file, launches a program, starts the computer, shuts it down, logs on, logs off, installs software, removes software, or attaches a flash drive, hard drives reflect those actions. Forensic analysts term such evidence 'artifacts.' Like archaeological artifacts

Digital evidence also differs from physical evidence in that, for most files, there is no way to know what data a file contains without opening it, meaning that desired data may be located in any part of the digital media or organizational structure. Indeed, data stored on a computer hard drive may be physically located in multiples places on the drive, and it is unhelpful and often inaccurate to think of the data as being located at any particular "place" or "places." In the physical world, a handgun cannot be disguised as—and will not be mistaken for—a kitchen table, nor will it be found in a pill bottle. But in the virtual world, that kind of deception—or error—is possible. A picture file may be intentionally disguised as a text file, for example, by changing the extension of the file name or by including the picture in a Microsoft Word document, which would be properly saved as a .doc (or similar) file. A picture file may contain text information if, for example, the picture is of a page of a book. Sophisticated users can hide digital data in much more complex ways, including changing date and time metadata and encrypting files so that they cannot be opened. *See* Orin S. Kerr, *Executing Warrants for Digital Evidence: The case for use restrictions on nonresponsive data*, 48 Tex Tech L Rev 1, 16 (2015) ("Data can always be changed. Maybe the modification will be easy or maybe it will be hard. But it can always be done."). Similarly, information can be hidden unintentionally. Most of us have had the experience of neglecting to name or properly "save" a document, only to have it disappear into an obscure temporary file, with its sole identifier a number assigned by the software. And even those with limited computer skills can easily delete their internet search "history" on a particular internet browser,

---

> showing how people once lived, forensic artifacts show how computers were used. Log files show what software programs did. Virtual memory paging files can reveal what was once in memory. Temporary files and link files can reveal that someone created, opened, or saved particular files. When a user saves a file in Microsoft Word, for example, eight different files or folders are created, modified, or accessed in sixteen different steps, all occurring in less than a second. In Windows, a vast configuration database, called the 'registry,' is an evidence treasure chest, showing recent user commands, recent files opened, recent network drives accessed, recent web sites visited, whether USB flash drives were attached, what Wi-Fi wireless access points have been used, and more."

Goldfoot, 16 Berkeley J Crim L at 127-28 (2011) (footnotes omitted).

although evidence of those searches will likely remain elsewhere on the hard drive. A forensic examiner who locates intentionally (or unintentionally) hidden information on a computer likely has responded to clues, followed instincts, and pursued many dead ends before being successful. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv L Rev 531, 545 (2005) ("[G]ood forensic analysis is an art more than a science.").

For those reasons, commentators and courts sometimes refer to searches of computers in a criminal investigation as involving "two basic steps: the data acquisition phase and the data reduction phase." Kerr, 119 Harv L Rev at 547; *see also United States v. Stabile*, 633 F3d 219, 234 (3d Cir 2011), *cert den*, 565 US 942 (2011) (applying two step perspective). In the data acquisition phase, the warrant authorizes the police to search a location for a computer and to seize it. As we discuss below, that physical search and seizure must comply with constitutional requirements, including the usual particularity rules for describing the physical place to be searched and the computer to be seized. But, generally, the seized computer or data itself has not yet been determined to have any evidentiary value.[9]

In the data reduction phase, there is an examination ("search") of the digital data, this time by a forensic examiner, to identify the particular data that may be useful as evidence. Using the familiar analogy of searching for a needle in a haystack, "data acquisition refers to collecting the hay, and data reduction involves looking through the haystack for the needle." Kerr, 119 Harv L Rev at 547. Because, as noted earlier, the location or form of specific information on a computer often cannot be known before the computer is actually examined, examiners conducting a reasonable computer search ordinarily will be permitted to look widely on the computer's hard drive to ensure that all

[9] Our discussion here is limited to circumstances where police seek data or information stored in the computer or evidence of the use of the computer as a computer. The analysis would be different, of course, if a laptop computer had been used to assault a person physically or was alleged to have been stolen. In those cases, police might seize the computer to test for DNA or fingerprint evidence, rather than to search the hard drive, and the possible seizure of the computer would be for evidentiary purposes more akin to those involved in searches for and seizures of other "things."

material within the scope of the warrant is found. Goldfoot, 16 Berkley J Crim L at 141 (noting consensus among federal circuit courts permitting "human forensic examiners to look at every file, albeit briefly, to determine whether it is in the warrant's scope"; citing cases); *see Andresen v. Maryland,* 427 US 463, 482 n 11, 96 S Ct 2737, 49 L Ed 2d 627 (1976) (holding, in nondigital context, that warranted search of attorney's office for certain papers did not violate Fourth Amendment when executing officers "cursorily" examined "innocuous documents *** to determine whether they [were], in fact, among those papers authorized to be seized"). For that reason, courts generally have not required that warrants include specific search protocols or *ex ante* limitations on computer searches. *See Stabile*, 633 F3d at 238 ("[I]t would be folly for a search warrant to structure the mechanics of the search because imposing such limits would unduly restrict legitimate search objectives." (Internal quotation marks omitted.)); Wayne R. LaFave, 2 *Search and Seizure* § 4.10(d), 969 (5th ed 2012) (noting courts are "disinclined" to impose *ex ante* search limitations). Moreover, a magistrate presented with a search warrant request, often early in a criminal investigation, would have little basis to make an informed decision as to whether proposed protocols regarding the seizure and search of a computer are sufficient to protect constitutional privacy interests or impose a constitutionally unnecessary burden on a criminal investigation. *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure,* 96 Va L Rev 1241, 1293 (2010) ("The factual vacuum of *ex ante* and *ex parte* decisionmaking leads such restrictions to introduce constitutional errors that inadvertently prohibit reasonable search and seizure practices.").

Finally, the novel nature of digital devices has led courts to apply search and seizure principles to those devices in a manner somewhat different from other physical evidence. The Supreme Court addressed some of those issues in *Riley v. California*, ___ US ___, 134 S Ct 2473, 189 L Ed 2d 430 (2014), and we discuss that case as background, because many of the parties' arguments in this case about searches of digital devices also were raised there.

In *Riley,* the Court considered a petitioner's postconviction challenge to the warrantless search of his "smart

phone" that police officers found in his pocket at the time of his arrest following a traffic stop and that they later examined at the police station.[10] *Id.* at 2480-81. The police found, among other things, gang-affiliated material and a photo of the defendant with a car linked to a shooting; the evidence ultimately supported his conviction for three crimes, including attempted murder, that were unrelated to the initial arrest. *Id.* at 2481. The government argued that, because the phone had been lawfully seized when the defendant was arrested, any information on the phone also was legitimately seized and could be used at trial. The government suggested that a search of all data on a cell phone was "materially indistinguishable" from searches of other physical items that might be found in a defendant's pocket. *Id.* at 2488.

The Court rejected that argument:

> "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. *** 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."

Id. at 2488-89. The Court identified the several ways in which cell phones "differ in both a quantitative and a qualitative sense" from other objects that might be found on an arrestee's person—and many of those characteristics also describe defendant's computer here. *Id.* at 2489.

The Court noted that the "immense storage capacity" of cell phones means that the physical limitation on

---

[10] *Riley* consisted of two consolidated cases, one involving a "smart phone" and the other a "flip phone." *Riley*, 134 S Ct at 2480-81. The Court used the term "cell phone" to encompass both, and we follow that usage in discussing the case. The Court noted that many cell phones "are in fact minicomputers." *Id.* at 2489. We agree that different species of personal digital devices, such as tablets, smart phones, laptops, and desktop computers, share many of the attributes discussed in *Riley*. As the state points out, treating some digital devices—such as the phones in *Riley* and the computers here—as unlike other "things" for some constitutional purposes requires determining whether a specific digital device falls within the category of items that must be seized and searched pursuant to the rules discussed in this opinion. We leave to future cases the determination of the specific boundaries of that category.

the amount of information a person could carry no longer applied. *Id.* A large storage capacity means that even a single category of information, such as emails or photographs, can "convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet." *Id.* Further, a cell phone collects "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." *Id.* Internet history can reveal "an individual's private interests or concerns"; location data can show where a person has been; and apps on a phone may provide information about, for example, an individual's political views, addiction treatment, dating, buying and selling, pregnancy, budgeting, and communicating. *Id.* at 2490. The Court not only rejected the government's claim that a cell phone was more like a "thing" than a "place," it also stated that even treating a cell phone like a house is insufficient to protect the privacy interests that many individuals have in the information stored in their phones:

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

Id. at 2491 (emphasis in original).

The Court explained that the development of the cell phone had undermined assumptions supporting the incident to arrest exception to the warrant requirement; with a cell phone, an arrestee could be carrying the equivalent of all the information in his house, or more. Therefore, the Court held that the exception could not be used to justify the search of cell phones, and it instead directed officers seeking to examine the contents of a cell phone to "get a warrant." *Id.* at 2495.

In this case, of course, the officers had a warrant, and we return to the facts here and the question of the validity of the warrant and the search of defendant's computer.

III. MAY THE AFFIDAVIT BE CONSIDERED WITH THE WARRANT?

We first address the issue of whether the information contained in Rookhuyzen's affidavit is properly considered part of the warrant itself. In the Court of Appeals, the state asserted that the affidavit was "attached to and referenced by" the warrant and, as a result, the court should consider the contents of the affidavit as part of the warrant in deciding defendant's challenge to the warrant's facial validity. In his response, defendant agreed that an affidavit may be considered part of the warrant if it physically accompanies the warrant and the warrant explicitly incorporates it by reference; however, defendant disputed that the state had established that the warrant here met those requirements, and, therefore, he claimed that the contents of the affidavit should not be considered.[11]

The Court of Appeals observed that, when a search is conducted pursuant to a warrant, the defendant bears "the burden of establishing facts pertaining to his 'challenge [to] the validity of the warrant itself.'" *Mansor*, 279 Or App at 790 (quoting *Walker*, 350 Or at 555 (brackets in *Mansor*)). Here, the state's contention that the affidavit was attached to and referenced in the warrant at the time of execution was supported, as the Court of Appeals said, by "permissible, albeit hardly indubitable, inference." *Id.* Defendant presented no evidence to controvert that inference. *Id.* On that record, the Court of Appeals concluded that defendant fell short of his burden of production and therefore considered the affidavit to be part of the warrant for purposes of its review.

We agree with the Court of Appeals that defendant failed in the trial court to establish the factual basis for his argument on appeal; for purposes of this case, we consider the text of the affidavit to be part of the warrant. That said, we note that parties may spend substantial time litigating whether the contents of an affidavit should be considered in

[11] The warrant did not contain the word "affidavit." It did, however, reference "Attachment A," which was a separate document listing items to be seized. The state presented evidence, which defendant did not controvert, that the affidavit was stapled to "Attachment A."

a challenge to a warrant. *See* LaFave, 2 *Search and Seizure* § 4.6(1) at 778 (noting a "great variety of viewpoints" on the issue). In our view, rather than relying on indirect inferences to establish a connection between the warrant and an affidavit, the better practice is for the warrant to include specific text from the affidavit or to incorporate the affidavit by express reference in the warrant. Merely attaching the affidavit or an exhibit with an attached affidavit to the warrant, without some textual reference, creates the ambiguous situation apparently present here. Moreover, as we discuss in greater detail below, in order to guide the persons conducting the forensic examination of a properly seized computer, the warrant itself should describe, with as much specificity as reasonably possible, the category or categories of information to be searched for on the computer, including, if available and relevant, the time period when the information was created, accessed, or otherwise used. That description, of course, must be based on affidavits or other record evidence that establishes probable cause to search the computer for such information.

Because we have concluded that the affidavit should be considered as part of the warrant in this case, it follows that the contents of the affidavit assist us in determining the scope of the search that the warrant permitted. The warrant itself authorized police to "seize and search and forensically examine" certain items listed in an attachment, and the listed items included defendant's computers. The affidavit also referred to, and sought authority to search for and seize, those items, and an exhibit to the affidavit refers to "items to be searched for, to be seized, and to be analyzed." The only reference in the affidavit to relevant information that Rookhuyzen believed was on the computer was the paragraph set out above, 363 Or at 190 (and one related sentence in the affidavit), regarding defendant's statements about searching the internet for first aid advice in the 15 minutes before he made the 9-1-1 call. Although the warrant, supplemented by the affidavit, authorized the "search," "analy[sis]," and "forensic[] examinat[ion]" of all the items seized, including the computers, the only description of any relevant information that Rookhuyzen believed might be found on the computers was that of the June 12

internet search history. We therefore view that description of the information to be searched for as a limitation on the search, analysis, and forensic examination authorized by the warrant.[12]

IV. IS THE WARRANT VALID?

A. *Search and Seizure Principles and History*

This case raises questions under Article I, section 9, of the specificity with which a warrant must describe the digital information that the state seeks, the search that the state may conduct, and the evidence that the state may use when police have probable cause to believe that a computer contains information related to a crime. Those questions implicate fundamental issues of personal privacy and the state's responsibility to prosecute crime in the novel and rapidly evolving context of digital evidence. Although this court previously has addressed the application of Article I, section 9, to some types of electronic evidence, we have not yet considered the application of the constitutional principles to the unique characteristics of a personal computer.

To do so, "we consider the 'specific wording of Article I, section 9, the case law surrounding it, and the historical circumstances that led to its creation.'" *State v. Carter*, 342 Or 39, 42, 147 P3d 1151 (2006) (quoting *Priest v. Pearce*, 314 Or 411, 415-16, 840 P2d 65 (1992) (brackets omitted)). The purpose of the historical analysis required under *Priest* is not to "freeze" the meaning of the state constitution at the time of its adoption. *State v. Davis*, 350 Or 440, 446, 256 P3d 1075 (2011). "Rather it is to identify, in light of the meaning understood by the framers, relevant underlying principles that may inform our application of the constitutional text to modern circumstances." *Id.*

Article I, section 9, of the Oregon Constitution provides:

> "No law shall violate the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search, or seizure; and no warrant shall issue but

[12] Unless the context indicates otherwise, when we refer to the "warrant" in the remainder of this opinion, we mean the warrant, as supplemented by the affidavit.

> upon probable cause, supported by oath, or affirmation, and particularly describing the place to be searched, and the person or thing to be seized."

Using that text as a starting point, we review this court's Article I, section 9, case law and our earlier discussions of historical circumstances. We consider whether the unique characteristics of computers make them unlike other "things" that may be seized. Then we determine what it means to "particularly describ[e] *** [the] thing to be seized" in the warrant, when that "thing" is information on a computer. Finally, we apply the results of our discussion to the facts of this case.

The text and principles of Article I, section 9, can be traced directly to the Fourth Amendment to the United States Constitution, and from there to state constitutional documents dating to the American Revolution. *See State v. Bridewell*, 306 Or 231, 241, 759 P2d 1054 (1988) (Peterson, C.J., concurring in part, dissenting in part) (discussing history of Article I, section 9); *see also* Jack L. Landau, *The Search for the Meaning of Oregon's Search and Seizure Clause*, 87 Or L Rev 819, 836-840 (2008) (recounting the origins of Article I, section 9). Those provisions themselves were, among other things, reactions to abusive "general warrants" of the English colonial government, which gave government agents "unlimited authority to search and seize." *State v. Blackburn/Barber*, 266 Or 28, 34, 511 P2d 381 (1973) (explaining that a historical motivation for Article I, section 9, was a fear of general warrants); *see also* Landau, 87 Or L Rev at 822-23 ("'General warrants' referred to writs that authorized the bearer to search unspecified places or arrest persons suspected of having been involved with a criminal offense."); Laura K. Donohue, *The Original Fourth Amendment*, 83 U Chi L Rev 1181 (2016) (relating the role of general warrants in the framers' development of the Fourth Amendment).

As we have previously explained, "[t]he privacy interests protected from unreasonable searches under Article I, section 9, are defined by an objective test of whether the government's conduct 'would significantly impair an

individual's interest in freedom from scrutiny, *i.e.*, his privacy.'" *State v. Wacker*, 317 Or 419, 425, 856 P2d 1029 (1993) (quoting *State v. Dixson/Digby*, 307 Or 195, 211, 766 P2d 1015 (1988)). Because "private *space* and privacy *interests* often are inextricably intertwined[,] *** privacy interests that are protected by Article I, section 9, commonly are circumscribed by the space in which they exist and, more particularly, by the barriers to public entry (physical and sensory) that define that private space." *State v. Smith*, 327 Or 366, 372-73, 963 P2d 642 (1998) (emphasis in original). At the same time, we have recognized that Article I, section 9, "must be read in light of the ever-expanding capacity of individuals and the government to gather information by technological means." *Id.* at 373. That is, Article I, section 9, applies to "every possible form of invasion—physical, electronic, technological, and the like." *Id.* We discuss the permissible scope of that legal intrusion below.

B. *Search for and Seizure of Computers*

1. *Seizure of the computers*

We begin by considering briefly the search for and seizure of defendant's computers themselves. Although defendant's motion to suppress challenged the seizure of the computers as well as the forensic examination of the computers for evidence and the use of that evidence at trial, defendant no longer argues that the seizure of the physical computers violated Article I, section 9. That argument would fail in any event. The warrant recounted defendant's statements to Rookhuysen about his internet searches, identified two laptop computers and two desktop computer towers in the apartment, and included statements by Rookhuyzen about how internet search engines are used to seek information (as defendant stated that he had done when B was not breathing) and about the need to have an examination conducted by a trained computer forensic examiner. The warrant was sufficiently particular in its description of the computers to be seized and the grounds for believing that evidence related to the criminal investigation was likely to be found on one or more of them to meet the particularity requirement of Article I, section 9, with respect to the seizure of the computers.

2. *Search of a lawfully seized computer*

The more difficult issue is whether the warrant's authorization of lawful seizure of the computers similarly authorized the state to conduct a search of the computers to locate and seize information or data on the computers for evidence of a crime. The principles underlying Article I, section 9, establish that an individual generally has a privacy interest in the information on his or her personal computer. A computer often is either located in a private space, such as a home, or secured by a password or biometric identification, or both. Those "barriers to public entry" are the sort contemplated in *Smith*, 327 Or at 373, that indicate the presence of constitutionally protected privacy interests. The state does not disagree. The state argues, however, that if police obtain a valid warrant to search for and seize a computer, they are "free to examine it as they see fit." The state asserts that "a computer is a thing, and a warrant to examine it need only identify the particular computer, not the data that the examination is intended to find." The state relies on cases involving other "things" seized in warranted searches and argues that once a "thing" is seized and examined for any purpose, "any privacy interest in that object is destroyed, and no purpose would be served by further limitation on the nature of examinations that may be performed on the object."

We agree with defendant and the Court of Appeals that the state's argument is not well taken. For reasons that we will explain, the fact that police have a warrant, based on probable cause, to search for and seize "things," including computers, does not necessarily mean that they may conduct a comprehensive forensic examination of a computer that they seize, and then use at trial anything they find on the computer, without limit.

As noted, the state accepts that individuals have a protected privacy interest in their computers and the information on them. The state's legal argument, however, fails to account for the fact that, unlike most other "things" that may be seized in a search, a computer or other digital device is a repository with a historically unprecedented capacity to collect and store a diverse and vast array of personal information. Moreover, that information is stored in

a manner that ordinarily makes it inaccessible to others. We discussed in detail above the reasons that computers and digital devices are different from most other "things" that can be seized in the course of criminal investigations and the Supreme Court's recognition in *Riley* that different search and seizure rules apply to those devices than to other "things." Indeed, the state's argument here is similar to the argument that the government made in *Riley* and that the Supreme Court rejected: If the item (the phone or computer) is lawfully seized, then any information that can be discovered within the item also is legitimately seized and can be used at trial. Although *Riley* involved a warrantless search incident to arrest and this case involves a computer seized pursuant to a warrant, defendant urges us to follow the Court's approach in *Riley* and hold that computers deserve more protection than other "things" under Article I, section 9.

The state argues that this court has previously held that an individual retains no privacy interest in storage media that is lawfully in the possession of the police. In *State v. Munro*, 339 Or 545, 124 P3d 1221 (2005), the police raided a home pursuant to a warrant in connection with a drug investigation and seized a beta format videotape and various contraband. The defendant was prosecuted for possession of the other contraband, but the videotape appeared to be blank. About a year later, acting on new information, police were able to view the contents of the tape, discovered that it contained child pornography, and prosecuted defendant based on that evidence. The defendant challenged the later examination of the tape—which the state conceded was a "search"—as violating Article I, section 9. This court held that no violation had occurred, because "[o]nce the police seized the videotape under the authority of the warrant, any privacy interest that defendant had in the contents of the videotape was destroyed by the authority of the warrant permitting the examination and exhibition of the contents of the videotape." *Id*. at 552.

The state erroneously assumes, however, that the videotape in *Munro* is analogous to a computer or a cell phone. Of the unique characteristics of the cell phone described in

Riley—such as containing many types of information, having immense storage capacity, and playing a role in many aspects of life—a videotape has none. In contrast with a cell phone, which continually creates and stores data as it is used, the only possible "search" of a videotape is for the police to view the tape as it was recorded. *Munro* held only that a single analog videotape is a "thing" for purposes of search and seizure analysis, and once it was seized pursuant to a valid warrant, the owner lost all privacy interest in it. That holding does not assist the state here.

Further, the state's semantic observation that a computer is literally a "thing" is a truism that does not compel a legal conclusion. And the state provides no persuasive rejoinder to the Court's description in *Riley* of the technological changes that led the Court to exempt cell phones from the "search incident to arrest" doctrine. The data contained on a personal computer is qualitatively and quantitatively different from the sort of information that could be found in other single objects, or even an entire house not containing digital data. *See Riley*, 134 S Ct at 2491. We reject the state's argument that a computer is merely a "thing to be seized" and that, once lawfully seized, the state is free to analyze or examine the computer without limit and to use any information that is found.[13]

We observe at this point that the state does not rely on the plain view doctrine—or any other exception to the warrant requirement—to justify the seizure and use at trial of information from defendant's computer; instead, its remaining arguments, which we discuss in detail below, turn on the scope of the warrant. The plain view doctrine permits police to seize evidence without a warrant if they are in a place where they have a right to be and have probable cause to believe that the evidence that they see in "plain

[13] We do not intend our discussion here of forensic examinations of computer hard drives to call into question our "container" decisions, although the underlying Article I, section 9, principles are at least similar, if not the same. *See State v. Heckathorne,* 347 Or 474, 481-85, 223 P3d 1034 (2009) (discussing cases). As we have emphasized throughout this opinion, because of (1) the vast and diverse information that may be stored on a computer, and (2) the fact that the search of a computer necessarily will discover information beyond that being searched for, the rules that we articulate for applying Article I, section 9, to computer searches will not necessarily be appropriate in other contexts.

view" is contraband or evidence of a crime. *Carter,* 342 Or at 45. A number of courts have considered the application of the plain view doctrine in computer search cases, and the cases are divided. *Compare United States v. Williams,* 592 F3d 511, 521-24 (4th Cir 2010), *cert den*, 562 US 1044 (2010) (admitting computer search data under plain view doctrine) *with Comprehensive Drug Testing, Inc.*, 621 F3d at 1170 (rejecting application of plain view doctrine as "too clever by half"). Commentators also have expressed differing views. *Compare* Kerr, 119 Harv L Rev at 577 (rejecting plain view in computer search cases) *with* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A perspective and a primer*, 75 Miss L J 193, 262 (2005) (approving plain view, citing cases). Moreover, it is not clear how a doctrine developed in connection with physical objects, the "incriminating character" of which must be "immediately apparent," *Minnesota v. Dickerson*, 508 US 366, 375, 113 S Ct 2130, 124 L Ed 2d 334 (1993), would apply to bits and files digitally stored on a computer hard drive.

We recognize that some of the legal conclusions that we reach in this case likely would have implications for a plain view argument, if raised in a computer search case. However, as noted, the state does not rely on that doctrine here and neither party has briefed the issue; in these circumstances, further discussion regarding the application *vel non* of that doctrine to computer searches should await a future case.

3. *The particularity requirement as applied to computer searches*

Our conclusion that the lawful seizure of defendant's computer does not, by itself, permit the state to analyze and use all of the information found on the computer leaves us with the task of considering the scope of the warrant and defendant's argument that the warrant was impermissibly overbroad. That task requires us to apply the particularity requirement of Article I, section 9, to the search of the computer's contents. We sketch the particularity requirement as set out in our prior cases, and then discuss that standard as it applies here.

A search warrant must "particularly describ[e] the place to be searched, and the person or thing to be seized." Or Const, Art I, § 9. Regarding places, the particularity requirement exists to "narrow the scope of the search to those premises for which a magistrate has found probable cause to authorize the search." *State v. Trax*, 335 Or 597, 602, 75 P3d 440 (2003) (quoting *State v. Cortman*, 251 Or 566, 569, 446 P2d 681 (1968), *cert den*, 394 US 951 (1969)). It is satisfied if the warrant "permits the executing officer 'to locate with reasonable effort the premises to be searched.'" *Trax*, 335 Or at 603 (quoting *Cortman*, 251 Or at 568-69). We have decided fewer cases that address the particularity requirement as it applies to the "thing to be seized." The doctrine in that area is highly fact dependent and eludes a single, concrete articulation. *See* LaFave, 2 *Search and Seizure* § 4.6(a) at 769-75 (listing 12 principles as "useful guideposts" in determining if a description of an item meets the Fourth Amendment particularity requirement). But the purposes of the particularity requirement as to things are the same for the requirement of particularity as to places, *viz.*: The warrant must allow the executing officer to identify with "reasonable effort" the things to be seized "for which a magistrate has found probable cause." *Trax*, 335 Or at 602-03.

Our cases have identified two related, but distinct, concepts that inform the particularity analysis—specificity and overbreadth. *See Mansor*, 279 Or App at 792-802 (discussing and applying specificity and overbreadth concepts). A warrant must be sufficiently specific in describing the items to be seized and examined that the officers can, "with reasonable effort ascertain" those items to a "reasonable degree of certainty." *Blackburn/Barber*, 266 Or at 35. But, even if the warrant is sufficiently specific, it must not authorize a search that is "broader than the supporting affidavit supplies probable cause to justify." *State v. Reid*, 319 Or 65, 71, 872 P2d 416 (1994).

The state argues that a warrant is sufficiently specific and not overbroad—and therefore satisfies the particularity requirement—if the warrant identifies the crime being investigated. It asserts that the warrant here

met that requirement because it referred to the crimes under investigation at the time the warrant was issued—criminal mistreatment and assault. Defendant responds that, for purposes of the search of a computer, the particularity requirement means that the warrant must identify (1) "a specific file or type of evidence supported by probable cause," (2) "a specific location on [the] computer," and (3) a specific time period, consistent with the probable cause justifying the warrant—essentially, the "what," the "where," and the "when" of the data or information that police have probable cause to search for on the computer.

Turning first to the state's argument that the warrant here was sufficiently particular because it authorized the search of the computer for "evidence of a particular crime," we disagree. The state suggests that we previously held in *State v. Farrar*, 309 Or 132, 149-50, 786 P2d 161, *cert den*, 498 US 879 (1990), that a search warrant was sufficiently particular if it referred to the crime under investigation. The warrants there instructed officers to search identified locations for a number of specific items and "any other physical evidence of the aggravated murder of [the victim]." *Id.* at 149. We explained that the warrants—and the phrase "any other physical evidence of the aggravated murder" as a description of the scope of the search—were valid because *former* ORS 133.585 (1973), *repealed by* Or Laws 1997, ch 313, § 37, authorized the seizure of items not specifically described in a warrant. *Id.* at 151. The applicable statute allowed officers searching a person or place to seize "things, not specified in the warrant, which the officer has probable cause to believe to be subject to seizure," articulating a version of the "plain view" exception to the warrant requirement.[14] *Id.* (quoting *former* ORS 133.585(1973)). That statute applied in the circumstances of that case, the court explained, because the officers knew the instrumentality of the crime and several related items that they were looking for—the murder weapon, stolen jewelry—but did not know if other physical evidence linking the defendant to the crime might be present in the locations they were authorized to search. *Id.*

[14] *See State v. Reger,* 277 Or App 81, 92 n 2, 372 P3d 26, *rev den,* 359 Or 847 (2016) (describing *former* ORS 133.585 (1973) as relating to one aspect of plain view doctrine and explaining repeal of statute).

Farrar thus did not turn on the fact that the warrants at issue there identified a particular crime. Rather, that decision was based on the court's determinations, first, that seizing the numerous specific physical items identified in the warrants (as to which there was probable cause) was permissible, and, second, that seizing other physical items related to the charged crime that officers might find in plain view as they conducted the warranted searches was permissible under the catch-all provision codified in *former* ORS 133.585 (1990). *Farrar* was a case-specific application of a statute (later repealed) and essentially upheld a search based on probable cause as described in a detailed affidavit and warrants. This court's statements in *Farrar,* quoted above, are not a blanket endorsement of nonspecific terms in search warrants and provide 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.

Defendant's proposed rules for determining when a search warrant for a computer is sufficiently particular are closer to the mark, although not without their own difficulties, which arise primarily because the particularity requirement developed in a world of physical evidence rather than in the digital context described above. We discuss that context and the Delaware Supreme Court's decision in *Wheeler,* and then evaluate defendant's argument that to meet the particularity requirement of Article I, section 9, a warrant to search a computer must identify the "what," the "where," and the "when" of the evidence that police seek.

The unique characteristics of computers, outlined above, have implications for the application of the particularity requirement as it applies to computer searches. In the physical world, "different spatial regions are used for different purposes," which allows police and courts to make probable cause determinations "as to where evidence may or may not be found." Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum L Rev 279, 303 (2005). Inside computers, however, there is "no way to know ahead of time where *** a particular file or piece of information may be located." *Id.* As a result, although the particularity

doctrine is an effective means of restraining the state's power to search and can protect against general warrants in the physical world, "the particularity requirement presents difficult challenges in the context of computer searches." *Wheeler*, 135 A3d at 299 (emphasis omitted; capitalization corrected); *see also* Kerr, 48 Tex Tech L Rev at 17 (concluding that "particularity alone is unlikely to provide sufficient limits on computer warrant searches").

In *Wheeler*, the Delaware Supreme Court reversed convictions for possession of digital child pornography because the material was found pursuant to an unconstitutionally overbroad warrant. The warrant authorized an unrestricted search of a defendant's computer and other digital equipment as part of an investigation into the defendant's alleged witness tampering. 135 A3d at 289. The evidence of the witness tampering was suspected to be a kind of "text" file, but the examiner did not use an available feature of the forensic software to limit his view to text-type files. *Id.* at 290. Instead, he viewed all file types and found, but did not open, video files with titles suggesting that they depicted child pornography. Based on those video files, the state obtained another search warrant authorizing the search of digital media already in its possession for evidence of child pornography, leading to the defendant's conviction. *Id.* at 291.

In holding that the first warrant was not sufficiently particular, the court stated that the warrant, by purporting to authorize an unlimited examination of the defendant's digital media, paved the way for "unconstitutional exploratory rummaging." *Id.* at 305. Notably, the court did not rest its invalidation of the warrant on the executing officer's failure to exclude nontext video files from the examination—as discussed above, such court-prescribed "search protocols" are, in the majority view, unworkable. Rather, the warrant was unconstitutionally overbroad because it "fail[ed] to limit the search to the relevant time frame." *Id.* at 304. Some federal and state courts have held that a warrant for a computer search is insufficiently particular if it does not include a temporal description of the evidence sought, in cases where relevant time information is available to the police. *Id.* at 304 n 117, 305 n 118 (citing cases). In addition,

the warrant expressly authorized the seizure and examination of all digital equipment, including video DVDs and digital cameras, despite the absence of any indication that those objects would contain textual evidence of witness tampering. *Id.* at 306. In all, the court declined to "prescribe rigid rules" governing the application of the particularity requirement in computer search contexts; rather, it concluded that a warrant "must describe what investigating officers believe will be found on electronic devices with as much specificity as possible under the circumstances." *Id.* at 304.

We return to the components of defendant's proposed rule. Following *Wheeler*—and, indeed, general principles of search and seizure law—we agree that to satisfy the particularity requirement, a warrant must describe, with as much specificity as reasonably possible under the circumstances, *what* investigating officers believe will be found on the electronic devices. *See id.* Defendant clarifies that that element does not necessarily mean the type of computer file, such as an email, text, or photograph. Rather, for the reasons discussed above regarding the nature of digital evidence, the "what" is a description of the *information* related to the alleged criminal conduct which there is probable cause to believe will be found on the computer. Given the protean variety of factual settings in which such warrants are likely to be sought, it would be a fool's errand to set out, in the abstract, detailed guidelines for determining how specific the "what" of the search must be to meet the particularity requirement of Article I, section 9, in the computer search context, and we decline to do so.

Defendant also argues that, to be sufficiently particular, a warrant authorizing a computer search must identify "where" the search may be conducted on the computer. Defendant contends that any search must be limited to "the place or specific location in the computer where the evidence is likely to be found without much effort or rummaging—in this case, defendant's 'internet browsing history.'" Defendant suggests that locations on a computer hard drive are like rooms in a house, and that the warrant must limit the search to specified rooms, such as "internet browsing history, document files, hard drive, emails, call logs, and varying application folders." We disagree.

It is certainly true that many warrants authorizing computer searches will identify commonly used software programs—email clients, internet browsers, document management tools—where relevant evidence is likely to be found. For the practical reasons explained above, however, a search warrant may be sufficiently particular without being limited to searching in those "places." Imposing such limits on a computer search would require police and the reviewing magistrate to know the technological specifications, including the configuration of the operating system and applications software on a computer, before a warrant could be obtained. Limiting a search to certain "places" on a computer, defined in terms of the computer's internal organization, such as the "My Documents" folder, is an *ex ante* limitation on the search. Such *ex ante* limitations would require a valid warrant to be based on more detailed knowledge of a specific computer and its software than would be required to meet the usual probable cause standard for the information being sought. And defining "places" on a computer in terms of a person's particular use of them, such as "places where a user may store documents," is essentially redundant of the "what" element discussed above. Moreover, information on a computer easily can be moved from one virtual location to another, either intentionally or by mistake. We do not think that it is useful to conceive of a computer as consisting of multiple "rooms" or containers, and a valid warrant to search a computer need not identify "places" to search at that level of abstraction.

Defendant also argues that a warrant for a computer search should include a "temporal limitation" or "when" requirement, if one is available and relevant. In *Wheeler*, the court held that the warrant was unconstitutionally broad because, among other things, it failed to "limit the search to the relevant time frame." 135 A3d at 304. In reaching that conclusion, the court noted that federal and state courts have concluded that "warrants lacking temporal constraints, where relevant dates are available to the police, are insufficiently particular." *Id.* at 304 n 117, 305 n 118 (listing cases). Certainly, consideration of the time when relevant documents were created or internet sites visited can be helpful in ensuring that the warrant describes

that which the executing officers may search for with sufficient specificity, but without impermissible overbreadth. And we agree with the reasoning in *Wheeler* and the cases cited there that when a time-based description of the information sought on a computer is relevant and available to the police, it ordinarily should be set out in the affidavit, and the warrant should include that description. That said, analytically, "temporal limitations" are more accurately seen as a way of identifying with greater specificity the "what" that is being searched for, rather than as a separate, independently required element, in meeting the particularity requirement for a computer search.

We thus agree in substantial part with defendant. The warrant to search a computer must be based on affidavits that establish probable cause to believe that the computer contains information relevant to the criminal investigation. To meet the particularity requirement of Article I, section 9, the warrant must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if relevant and available, the time period during which that information was created, accessed, or otherwise used. We emphasize, however, based on our discussion of digital devices and computer searches above, *see* 363 Or at 197-202, that the forensic examination likely will need to examine, at least briefly, some information or data beyond that identified in the warrant.[15]

4. *Was the warrant here sufficiently particular?*

Returning to the facts of this case, the affidavit established probable cause to believe that child abuse was the cause of B's injuries and probable cause to believe that evidence related to the crime would be found on the computer. When Rookhuyzen interviewed defendant in his apartment, defendant was "completely non-emotive" and had not called his wife, behavior that Rookhuyzen called "highly" and "extremely" unusual. Based on defendant's statements regarding his searches shortly before the 9-1-1 call, there also was probable cause to believe that one or

[15] To be clear, although a computer search may need to be broad, it must be reasonably executed. Or Const, Art I, § 9 (protecting right to be free from "unreasonable search, or seizure").

more of the computers at the apartment contained information that would confirm or refute defendant's statements about what happened in the minutes before that call:

> "[Defendant] told [Rookhuyzen] that he searched the internet between the time he noticed [B] was having difficulty breathing and the time he called emergency dispatch. He told [Rookhuyzen] that he was using a computer to search the internet for advice on what he should do."

Additionally, the affidavit recited statements of the pediatrician who examined B that B's injuries were "clearly the result of intentionally inflicted abuse" and that "[defendant's] version of events was not consistent with [B]'s condition"; that B had a brain injury "unrelated to choking"; and that B had a recent skull fracture and bilateral retinal hemorrhages. Finally, the affidavit stated Rookhuyzen's view, based on his training and experience, that computers retain a history of internet use and that examination of a computer needs to be done in a forensic laboratory.

The affidavit thus established probable cause to believe that a crime had occurred on June 12 and explained, based on case-specific facts and the officer's training and experience, that there was probable cause to believe that evidence relevant to the investigation would be found on the computer. The affidavit described with particularity certain evidence likely to be found on the computer. Indeed, as the Court of Appeals noted, defendant twice conceded at the suppression hearing "the lawfulness of a search of the computers with respect to the 15 minutes preceding the 9-1-1 call." *Mansor*, 279 Or App at 791.

The warrant, read in conjunction with and limited by the affidavit, met the particularity requirement of Article I, section 9, as we have articulated it above. It sufficiently described the "what" to be searched for and the relevant time frame: The June 12 internet search history. It informed those executing the warrant as to what they were to look for "with a reasonable degree of certainty." *Blackburn/Barber*, 266 Or at 35. And, because that description limited the extent of the search that was authorized by the warrant, as we read it, the permitted search was not "broader than the supporting affidavit supplie[d] probable cause to justify."

Reid, 319 Or at 71. For that reason, although we agree with much of the Court of Appeals' learned analysis, we disagree with its legal conclusion that the warrant was overbroad on its face and therefore invalid *in toto.* In our view, the warrant was not facially invalid because it authorized a search for only the June 12 internet history.

V. USE OF RESULTS OF COMPUTER SEARCHES

It does not follow, however, that the trial court was correct in denying defendant's motion to suppress the results of the forensic examination in their entirety. As we have discussed, the warrant authorized a search only for the June 12 internet search history. That search was supported by probable cause, was sufficiently specific, and was not overbroad. The nature of a computer search, however, means that, in searching for that history, that the forensic examiners were likely to come across or discover additional information. And, in this case, the forensic examination searched for and uncovered information, later used at trial, that went far beyond the scope of the warrant.

To ensure the protection of Article I, section 9, rights, we must consider what restrictions, if any, should be imposed on the use of information police obtain through reasonably executed warranted computer searches when those searches uncover evidence beyond that authorized in the warrant, and when no exception to the warrant requirement supports the collection or use of that evidence.

In our view, the privacy interests underlying Article I, section 9, are best protected by recognizing a necessary trade-off when the state searches a computer that has been lawfully seized. Even a reasonable search authorized by a valid warrant necessarily may require examination of at least some information that is beyond the scope of the warrant. Such state searches raise the possibility of computer search warrants becoming the digital equivalent of general warrants and of sanctioning the "undue rummaging that the particularity requirement was enacted to preclude." *Mansor,* 279 Or App at 803 (internal quotation marks omitted). Although such searches are lawful and appropriate, individual privacy interests preclude the state from benefiting from that necessity by being permitted to

use that evidence at trial. We thus conclude that the state should not be permitted to use information obtained in a computer search if the warrant did not authorize the search for that information, unless some other warrant exception applies. *See* Kerr, 48 Tex Tech L Rev at 24 (suggesting use restrictions for data "nonresponsive" to the warrant). Put differently, when the state conducts a reasonably targeted search of a person's computer for information pursuant to a warrant that properly identifies the information being sought, the state has not unreasonably invaded the person's privacy interest, and the state may use the information identified in the warrant in a prosecution or any other lawful manner. But when the state looks for other information or uncovers information that was not authorized by the warrant, Article I, section 9, prohibits the state from using that information at trial, unless it comes within an exception to the warrant requirement.

That approach is consistent with our explanation that the purpose of rules requiring the suppression of evidence gathered in violation of the constitution is to restore the parties to the position they would have been in had the violation not occurred:

> "[R]ules of law designed to protect citizens against unauthorized or illegal searches or seizures of their persons, property, or private effects are to be given effect by denying the state the use of evidence secured in violation of those rules against the persons whose rights were violated, or, in effect, by restoring the parties to their position as if the state's officers had remained within the limits of their authority."

State v. Davis, 295 Or 227, 237, 666 P2d 802 (1983). Here, the warrant authorized the police to search for specific information on defendant's computer—the June 12 internet search history. The state properly searched for and found that evidence and used it at trial. But the state also searched for and obtained, and used at trial, a substantial amount of evidence from the computer that was not within the scope of the warrant. We have rejected the state's arguments that the warrant authorized the seizure of that additional evidence, and the state has identified no exception to the warrant requirement that supported its acquisition, and use, of

that evidence. To restore defendant to the position he would have been in had the police not obtained that additional evidence, the evidence other than the June 12 internet search history should have been suppressed.

VI. CONCLUSION

In summary: Article I, section 9, prohibits general warrants that give "the bearer an unlimited authority to search and seize." *Carter*, 342 Or at 43 (quoting *Reid*, 319 Or at 69). Instead, subject to certain exceptions, that provision requires a warrant based on probable cause and describing with particularity that which the state may search for and seize. As the Supreme Court explained in *Riley*, digital information on cell phones—and, by logical extension, computers and similar digital devices—implicates privacy interests entitled to constitutional protection under the Fourth Amendment, and those interests are equal to or surpass those of a home. 134 S Ct at 2491. The Court's reasoning is persuasive and informs our understanding of the proper application of the Oregon warrant requirement to searches of computers and other digital devices.

As explained above, we reject the state's initial argument that a computer is like any other "thing" and that, if it is lawfully seized pursuant to a warrant or is otherwise lawfully in the state's possession, any information that is discovered on the computer is also lawfully seized and can be used at trial. We also reject the state's alternative argument that a warrant to seize and search a computer is sufficiently particular if it simply identifies the crime or crimes being investigated. We instead conclude that, to meet the particularity requirement of Article I, section 9, a warrant to search for and seize a computer—and to search the computer itself for information related to a crime—must be based on probable cause to believe that such evidence will be found on the computer and must describe the information the state seeks (the "what") with as much specificity as reasonably possible under the circumstances, including, if available and relevant, a temporal description of when the information was created, accessed, or otherwise used. As a practical matter, a forensic examination of the computer that reasonably seeks to discover the evidence described in

the warrant may reveal evidence that is beyond the scope of the warrant. We also hold that, because of the possibility that a computer search will uncover information that is not authorized by the warrant, a defendant's Article I, section 9, privacy rights prevent the state from using such information unless it comes within an exception to the warrant requirement.

In this case, the trial court denied defendant's motion to suppress the "material discovered as the result of a warranted search of his home computers." *Mansor*, 279 Or App at 779. The Court of Appeals reversed, holding that the warrant was impermissibly overbroad and that the trial court should have granted the motion to suppress. *Id.* at 802. As discussed at length above, we conclude that the warrant, as limited by the affidavit, was not facially invalid, because the accompanying affidavit established probable cause to search the computers and specifically identified the information to be sought. However, the warrant, as limited by the affidavit, did not authorize police to search for and recover much of the other voluminous material that was contained in the computer and that also was subject to the motion to suppress. The trial court's decision denying the motion to suppress and allowing the evidence beyond the scope of the warrant to be used at trial was erroneous. That error was not harmless. We therefore reverse and remand to the trial court for further proceedings consistent with this opinion.

The decision of the Court of Appeals is affirmed. The judgment of the circuit court is reversed, and the case is remanded to the circuit court for further proceedings.