# RECORD IMPOUNDED



SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-3144-21

STATE OF NEW JERSEY,

Plaintiff-Appellant,

v.

JEFFREY REITZ,

Defendant-Respondent.

———————————————

Argued November 16, 2022 – Decided February 17, 2023

Before Judges Accurso, Vernoia and Natali.

On appeal from an interlocutory order of the Superior Court of New Jersey, Law Division, Gloucester County, Indictment No. 21-09-0133.

Adam D. Klein, Deputy Attorney General, argued the cause for appellant (Matthew J. Platkin, Attorney General, attorney; Adam D. Klein, of counsel and on the brief).

Rocco C. Cipparone, Jr., argued the cause for respondent.

PER CURIAM

Defendant Jeffrey G. Reitz is charged in a superseding indictment with four counts of possession of child-sexual-exploitation/abuse-material (CSEAM) images, two counts of official misconduct, two counts of distribution of CSEAM images, and one count of attempted tampering with evidence.[1]

By leave granted, the State appeals from the trial court's order granting in part defendant's motion to suppress evidence — data files from three email accounts — seized pursuant to two communications data warrants (CDWs). Based on our review of the record, the parties' arguments, and the applicable legal principles, we vacate the court's order suppressing the State's evidence and remand for further proceedings.

I.

The charges against defendant arise out of an undercover investigation of J.W., who used an online computer service to offer her five-year-old

[1] Defendant is a New Jersey State Trooper. The official misconduct charges are based on claims defendant possessed CSEAM images and "refrained from reporting the distribution of said image[s], with the purpose to obtain a benefit for himself or another." The indictment also charges co-defendant Andrea Knox with possession of child sexual abuse material, attempted tampering with evidence, and official misconduct.

daughter K.H. for sexual encounters.[2] Following J.W.'s arrest on endangering-the-welfare-of-a-child charges, an extraction of data from her cellphone revealed communications with "glbmm2012@yahoo.com" (Glbmm), who expressed an interest in a sexual encounter with K.H. J.W. fulfilled Glbmm's request for images of K.H. with a photograph of the child's vagina. Glbmm communicated with J.W. during December 2014 and January 2015.

The data obtained from J.W.'s cellphone further revealed communications with Glbmm through a different email address and telephone number, both of which were identified as defendant's.

The State Obtains and Executes Three CDWs

In December 2018, the State obtained a CDW (CDW-1) for emails, texts, images, IP addresses, and other data "for the period of December 1, 2014 through January 31, 2015" for Yahoo accounts identified as being used by defendant. New Jersey Division of Criminal Justice detective Charles Pusloski executed CDW-1 and obtained data for the Yahoo accounts. The data included

[2] We employ initials to identify K.H. and her mother, J.W., to protect K.H.'s privacy and because the identity of an alleged victim of a sexual offense is excluded from public access under Rule 1:38-3(c)(12), and the identity of a child victim of sexual offenses, including endangering the welfare of a child under N.J.S.A. 2C:24-4, is excluded from public access under Rule 1:38-3(c)(9) and N.J.S.A. 2A:82-46.

the 2014-2015 email communications between defendant and J.W., including the photograph of K.H.'s vagina.

During his review of the data, Pusloski observed that emails sent from the Yahoo accounts originated from the sender's iPhone. Pusloski served Apple with a subpoena for device registration information, iCloud subscriber information, and iOS device activation information for defendant's name and telephone number. After Apple provided three email addresses associated with defendant's Apple accounts, the police arrested defendant, and Pusloski applied for a CDW for data and information related to the three email addresses.

On June 20, 2019, the court issued a CDW (CDW-2) for data from defendant's "Apple-linked account," including "all stored images," "communications emails and attachments," "subscriber name, address, and contact number," text messages, "photos and videos from any linked Apple device," "and any other iCloud or backup data for the period of December 1, 2014[,] through January 31, 2015." Thus, CDW-2 identified the data which the State was authorized to seize and search, and it limited that authority to a date range — "the period of December 1, 2014[,] through January 31, 2015."

Apple provided data responsive to CDW-2. In its written statement accompanying its production of the data, Apple advised it provided "true copies of the available data Apple has using the criteria and information provided in" the warrant. Apple also explained it was unable to "apply a date filter" in its production of certain of the data, "the iCloud backup data," stating:

> Please note that certain files within the iCloud backup data may contain aggregated data where Apple was unable to apply a date filter. Due to the complexity of the iCloud backup data you may need to work with a cellular forensics expert to access and review the provided data. Apple is unable to provide technical assistance.
>
> [(emphasis added).]

Thus, in its response to CDW-2, Apple represented it provided data "using the criteria" in the warrant — which we observe included a limited authorized date range — with one expressly limited exception, "certain files within the iCloud backup data." Pusloski reviewed the data without first consulting a cellular forensics expert generally or in accordance with Apple's suggestion he do so regarding the "iCloud backup data."

In a July 23, 2019 email to Apple, Pusloski stated he reviewed the data produced in response to CDW-2 and determined "[s]ome of the file creation

dates are outside the date range [December 1, 2014 through January 31, 2015] scope of the warrant." The letter did not indicate whether the "file creation dates" to which he referred were associated with data within the "iCloud backup data" or within other data files. Pusloski requested "guidance on why this is happening" and asked, "is Apple unable to provide date-specific files?" He also noted that despite the date range set forth in CDW-2, he saw two digital "photos of documents with dates in 2019" in the data Apple produced. One of the photographs is of a document dated "April 18, 2019." Apple did not respond to Pusloski's email.

Pusloski then applied for a third CDW seeking from Apple the same data covered by CDW-2 but for an expanded date range of December 1, 2014 to April 18, 2019. In his affidavit supporting the warrant request, Pusloski explained he sought data in the expanded date range in part because his review of the data Apple provided in response to CDW-2 included "five image files consistent with child pornography" in a folder "associated with [defendant's] account," as well as "pictures as part of the iCloud backup" files that appeared to be "images" of photos of a "computer screen [that] were consistent with

child pornography."[3] Pusloski further asserted he observed two digital photographs depicting "date-specific material that was outside the scope of the" December 1, 2014, through January 31, 2015 date range in CDW-2. He explained that immediately upon observing the two pictures, he "stopped reviewing the provided materials" and sought "an expanded [date range] scope search warrant, based on the production provided by Apple."

The court granted Pusloski's application and issued an August 21, 2019 CDW (CDW-3) directing that Apple produce the same data and information as specified in CDW-2, but with an expanded date range of December 1, 2014 to April 18, 2019. After obtaining CDW-3, Pusloski continued his review of the data provided in response to CDW-2. He also reviewed additional data produced by Apple in response to service of CDW-3, and determined it included files containing alleged child pornography the State claims defendant sent to an individual identified as his co-defendant Andrea Knox.

Following his review of the data produced in response to CDW-3, Pusloski send a second email to Apple stating that its response to CDW-2

[3] The motion record does not reflect whether those images fell within the date range authorized by CDW-2. Moreover, as we explain, the record does not include evidence establishing the manner and criteria by which the date of any data produced would be determined for purposes of analyzing whether the data fell within the authorized date range in CDW-2.

included photos "in the i[C]louds folder." The email further stated Apple's production of data in response to CDW-2 did not show any "pictures in that folder." Pusloski asked, "Why would the second request reveal no photos from that account?" There is no record Pusloski received a response to his inquiry.

In December 2019, a state grand jury indicted defendant on two counts of possession of child pornography. In a superseding indictment, the grand jury charged defendant with four counts of possession of child sexual abuse material, two counts of official misconduct, two counts of distribution of CSEAM, and one count of attempted tampering with evidence.

Defendant's Suppression Motion

Defendant moved to suppress the evidence seized pursuant to the three CDWs. In his briefs supporting the motion, defendant claimed Pusloski improperly exceeded the scope of the search authorized by CDW-2 by viewing data outside the warrant's authorized date range.[4] Defendant also argued the evidence derived from CDW-3 must be suppressed because that warrant was based on the data Pusloski improperly viewed outside the date range

[4] Defendant did not seek suppression of data within the CDW-2 date range that the State seized based on its review of the data supplied in response to CDW-2.

authorized by CDW-2 during his search of the data supplied by Apple in response to that warrant.[5]

In his briefs to the motion court, defendant relied on Pusloski's description of his search of the CDW-2 data set forth in his affidavit in support of CDW-3, and Pusloski's emails to Apple, as the factual bases for his claim that Pusloski's discovery of digital images outside CDW-2's date range impermissibly exceeded the scope of the warrant and was not otherwise supported under the plain view exception to the warrant requirement. More particularly, defendant argued Pusloski's description of his search of the data did not permit a finding that his discovery of the two photographs fell within the plain view exception because the digital photographs were outside CDW-2's date. See State v. Gonzales, 227 N.J. 77, 81 (2016) (explaining the plain view exception to the warrant requirement applies where "a police officer is

[5] In his briefs to the motion court, defendant made other arguments we do not address because they were rejected by the court and are not the subject of the State's pending interlocutory appeal. Those arguments include: the CDWs are not supported by sufficient probable cause and do not define the scope of the authorized searches with sufficient particularity; the affidavits supporting the applications for the CDWs lack sufficient information regarding defendant such that the State is entitled to the "presumption in child pornography cases that extends the staleness doctrine" for determining the reasonable time for a permissible search; and law enforcement attempted to search defendant's cellphone prior to obtaining a warrant and, as a result, the court should suppress any evidence obtained from the phone.

lawfully in the area where he observed the evidence [and] it is 'immediately apparent' that the item observed is evidence of a crime or contraband").

Defendant's briefs to the motion court also asserted Pusloski should have known the images included data outside the authorized date range because Apple's statement accompanying its production of data in response to CDW-2 warned certain files were not date-filtered, and Pusloski failed to confer with a cellular forensics expert prior to reviewing the data as recommended by Apple.

Defendant further asserted there is metadata associated with each data file, including files containing digital photographs, and Pusloski should have considered the metadata information prior to reviewing the data files to determine if they were within CDW-2's authorized date range.[6] Defendant asserted the metadata would have revealed whether a data file was within CDW-2's date range without the necessity of first opening the file and reviewing digital images in the file.

---

[6] "Metadata is information used by a computer to manage and often classify the origin and other attributes of a computer file." 1 Arkfield on Electronic Discovery and Evidence § 3.7; see also id. § 1.2 (noting "all . . . computer files" possess some form of metadata). Yet, the concept is expansive. Metadata may provide when a file was "written," "created," "modified," or "last accessed," among other properties. David T. Cox, Litigating Child Pornography and Obscenity Cases in the Internet Age, 4 J. Tech. L. & Pol'y 1, 108 (1999); Darrin J. Behr, Anti-Forensics: What It Is, What It Does and Why You Need to Know, 255 N.J. Law. 9, 13 (Dec. 2008).

The State filed a brief in opposition to defendant's motion, arguing the CDWs are presumed valid and are otherwise supported by the probable cause established in Pusloski's supporting affidavits. The State also argued Pusloski's description of his search of the data set forth in his affidavit in support of CDW-3 established the legality of the search of the data Apple produced in response to CDW-2.

The State asserted the data files supplied by Apple in response to CDW-2 did not include "temporal information" that could have been properly relied upon to determine if the data files, including the images and photographs, fell outside the authorized date range. The State also asserted, "[e]ven if a forensic examiner had reviewed the files, he or she would not have been able to tell if they were within the date range of [CDW-2] without opening them."

The State claimed Pusloski discovered the out-of-date-range images while he properly reviewed the data; he discontinued searching the data when he first observed images outside the date range; and he then immediately applied for a warrant, CDW-3, with an expanded date range. The State also claimed Pusloski observed the out-of-date-range data while conducting a search authorized by CDW-2 and his discovery of the data outside the

authorized date range therefore fell within the plain view exception to the warrant requirement.

At oral argument on the motion, defendant also relied on his counsel's arguments concerning the proper interpretation of Pusloski's July 23, 2019 email to Apple, claiming Pusloski's reference in the email to the "creation dates" of images he observed that fell outside CDW-2's date range was to the "metadata" associated with the images. Based on that premise, counsel argued Pusloski should have reviewed the metadata for each file before he opened a file and viewed a data file image, to determine if a file or image fell outside the authorized date range.

Counsel also disputed the State's claim a forensic examiner could not discern the creation date of a digital image by first reviewing the associated metadata. In fact, counsel asserted defendant's computer forensics expert would testify at the hearing that the data produced by Apple included "metadata from which someone who knows what they're looking for would . . . be able to see the creation dates of those files."

During the hearing, however, defendant's expert did not offer any testimony concerning metadata associated with the data produced by Apple in response to CDW-2, and the expert did not offer any opinion undermining the

State's claims concerning the digital properties of the data Pusloski reviewed. The expert's testimony was limited to an issue not pertinent to the State's interlocutory appeal — whether there was data on defendant's cellphone showing the State attempted to search the phone without a warrant.

The court originally scheduled the hearing on defendant's suppression motion for December 20, 2021. On that date, before the hearing commenced, both parties communicated to the court that they did not understand the scheduled proceeding would be an evidentiary hearing. Defense counsel believed the hearing was an arraignment, and the Deputy Attorney General (DAG) appearing on behalf of the State, for her part, did not "believe there [would] be an evidentiary hearing" at all, "as there [were] no disputes over relevant facts." Defense counsel disagreed, but indicated he was still reviewing the file. The court adjourned the hearing.

On March 4, 2022, the trial court heard the suppression motion. Defendant presented an expert witness in the field of computer forensics who, as noted, testified only that in his opinion data on defendant's cellphone established there were attempts to access the phone prior to the issuance of any warrants for the phone. The balance of the hearing consisted of the arguments of counsel.

Pertinent here, defense counsel argued the statements made by Pusloski in support of the application for CDW-3, explaining his review of the data supplied by Apple in response to CDW-2, as well as emails Pusloski sent to Apple following his review of the data supplied in response to CDW-2 and CDW-3, established Pusloski's review of the data provided in response to CDW-2 exceeded the authorized date range of the warrant. Counsel argued the trial court should suppress any data outside the CDW's date range that Pusloski observed during his review of the data provided in response to CDW-2. Counsel further argued all data obtained in response to CDW-3 should be suppressed because that warrant was based on data – the two digital photographs – Pusloski improperly viewed because they fell outside CDW-2's date range.

The State offered a different interpretation of Pusloski's statements made in support of CDW-3 to explain his discovery of the two photographs. The State requested an opportunity to call Pusloski to testify at a later date concerning his search of the data provided in response to CDW-2. During a colloquy with the court, the DAG stated:

> [I]t was my understanding that because there were no questions about the material facts of this case that this would be a legal argument only. If Your Honor would

> like to hear from him, we can certainly bring him in . . . at another time.

The colloquy then continued:

> THE COURT: . . . I'll leave that to you. If you wish us to give you another date that he can come in, I will certainly permit you to do that.
>
> [DAG]: And Your Honor, based on your questions then the [S]tate would be asking to bring him in, if you have questions regarding what is in the scope and what is outside the scope. I can't testify to what's in and what's outside the scope.

Defense counsel understood the State had requested a continuance to produce Pusloski as a witness. Defense counsel objected, arguing that granting the request would prejudice defendant by giving the State a "second bite of the apple." In response, the DAG reiterated her understanding the March 4, 2022 hearing was not to be an evidentiary hearing. The court did not directly address the DAG's request and instead determined it would hear the parties' legal arguments "and go from there." Counsel completed their arguments, and the court reserved decision on defendant's motion without further addressing the State's request to "bring [Pusloski] in" at a later date.

In its written decision, the court determined Pusloski's search of data produced in response to CDW-2 that fell outside the authorized date range was unconstitutional because it exceeded the scope of the warrant. The court also

found Pusloski's review of data — digital images — outside the authorized date range did not otherwise fall within the plain view exception to the warrant requirement.[7] The court suppressed all evidence derived from CDW-3 as fruit of the poisonous tree because the State's application for CDW-3 with an expanded date range was based on the unconstitutionally seized evidence from the execution of CDW-2. As noted, the court rejected all defendant's other arguments supporting the suppression motion.

The court entered an order denying the motion to suppress the evidence seized in response to CDW-1, granting the motion to suppress "[a]ll evidence outside the dates of . . . December 1, 2014 and January 31, 2015" derived from CDW-2, and granting the motion to suppress all evidence derived from CDW-3. We granted the State's motion for leave to appeal from the court's order.

The State Supplements the Record

Following our grant of the State's motion for leave to appeal, we also granted the State's motion to supplement the record with a certification from

[7] The court also determined Pusloski's viewing of data falling outside the date range authorized in CDW-2 did not fall within the "independent source" exception to the warrant requirement. See generally State v. Smith, 212 N.J. 365, 394-95 (2012) (explaining the elements of the independent source exception to the warrant requirement). The State does not address that determination in its brief on appeal. We therefore do not address it.

Pusloski, essentially in the form of a proffer of the testimony he would have given, providing information concerning his review of the data Apple supplied in response to CDW-2 and his discovery of the two digital photographs outside the warrant's date range.

Pusloski's certification describes his experience and training in the identification and seizure of digital evidence, the recovery of digital evidence, digital forensics, and computer crimes investigations. He also generally describes his involvement in the investigation that led to the charges against defendant, and his role in applying for, and executing, the three CDWs.

Pusloski explained the manner in which he reviewed the data, including digital images, produced by Apple in response to CDW-2. He stated he did not review any metadata associated with any of the data files because it is not shown on the digital images and it "can be manipulated, edited, or otherwise changed, and cannot reliably help determine when photographs were taken."

Pusloski stated that during his review of the data produced in response to CDW-2, he found images in some of the folders, but none "displayed dates or times." Some of the images depicted "several suspected CSEAM images, which [he] determined may have been case-related." As he continued to review images, he observed two photographs of documents that bore dates in

2019 — a calendar and an image of a document for "take your child to work" day. Upon seeing those documents, he immediately ceased his review of the CDW-2 data supplied by Apple.

He then sent the July 23, 2019 email to Apple stating "some of the file creation dates are outside the date range scope of the warrant." In his affidavit, Pusloski explained his reference to the "file creation dates" in the email did not refer to file creation dates that might have been gleaned from a review of metadata because he did not review metadata associated with any of the data Apple produced. Pusloski stated the email's reference to the "file creation dates" was only to the dates shown on the documents in the two photographs he reviewed immediately prior to discontinuing his search.

Pusloski further certified that neither he nor a "forensics-trained-law-enforcement-team" could determine when the CSEAM images he saw during his review of the CDW-2 production "came into existence." According to Pusloski, he determined the CDW-2 production included data outside the authorized date range "only because [he] unexpectedly saw the pictures of the two documents, which in the images themselves displayed the year 2019."

## II.

We consider on this interlocutory appeal only the State's challenge to the court's grant of defendant's motion to suppress the data, including images, produced by Apple in response to CDW-2 that falls outside the December 1, 2014 to January 31, 2015 date range, and all the data, including images, provided in response to CDW-3. We do not consider or express an opinion on the court's rejection of any of defendant's arguments supporting his suppression motion or on any portion of the court's order denying defendant's suppression motion.

Where a court holds an evidentiary hearing on a motion to suppress evidence, we are bound to uphold a trial court's factual findings if they are supported by "sufficient credible evidence in the record." State v. Lamb, 218 N.J. 300, 313 (2014). We are further obliged to defer to findings based on a motion court's "review of documentary or video evidence." State v. Carillo, 469 N.J. Super. 318, 332 (App. Div. 2021) (citing State v. S.S., 229 N.J. 360, 381 (2017)). We owe no deference to a court's findings that are based on the arguments of counsel or the unsupported "factual allegations in a brief." Id. at 333.

Rule 3:5-7(b) provides that where a defendant challenges a search conducted pursuant to warrant, the defendant must file a motion with a brief "stating the facts and arguments" upon which the defendant relies. The State is required to file a brief in response setting forth "the facts and the arguments in support of the search." R. 3:5-7(b). The Rule further authorizes the defendant to file a reply. Ibid.

There is no requirement the factual allegations set forth in the parties' respective briefs be supported by affidavits, certifications, or other competent evidence. See Carillo, 469 N.J. Super. at 332 (explaining "Rule 3:5-7 carves out an exception to Rule 1:6-6, which generally requires that evidence on motions be presented by affidavit or certification"). As a result, a court considering a motion to suppress evidence seized pursuant to a search warrant must determine whether there is a factual dispute requiring an evidentiary hearing based on an "examination of the factual assertions contained in the briefs of the parties." Id. at 333 (quoting State v. Torres, 154 N.J. Super. 169, 172 (App. Div. 1977)).

We do not accord deference to a court's decision that there is no need for an evidentiary hearing on a motion to suppress based on a determination, made after a review of the parties' briefs, that there are no "material facts" in dispute.

Ibid. "Determining . . . if facts are in dispute is a matter of law" that may be made by "examin[ing] side-by-side the parties' allegations." Ibid. The determination of whether facts are material also presents an issue of law we review de novo. Ibid.

A search "executed pursuant to a warrant is presumed to be valid and . . . a defendant challenging its validity has the burden to prove 'that there was no probable cause supporting the issuance of the warrant or that the search was otherwise unreasonable.'" State v. Keyes, 184 N.J. 541, 554 (2005) (quoting State v. Jones, 179 N.J. 377, 388 (2004)). Where the State claims a warrantless search is valid under a recognized exception to the warrant requirement, the State must present evidence establishing the elements of the exception claimed. See State v. Elders, 192 N.J. 224, 246 (2007) (quoting State v. Pineiro, 181 N.J. 13, 19-20 (2004)) (explaining the State "bears the burden of proving by a preponderance of the evidence that a warrantless search or seizure 'falls within one of the few well-delineated exceptions to the warrant requirement.'").

The State makes two arguments in support of its appeal. First, the State claims Pusloski's discovery of the photographs outside the CDW-2's date range falls within the plain view exception to the warrant requirement. Second, the

State asserts the court erred by failing to conduct a full evidentiary hearing on the disputes of fact presented by the parties' motion briefs, and, as a result of that failure, the court did not consider or decide "whether [Pusloski's] viewing of the iCloud folder of photographs impermissibly broadened CDW-2, whether the CSEAM images fell outside CDW-2's scope, and, if so, whether an exception to the warrant requirement applies." Included within the State's latter claim is the contention the court erred by denying the DAG's request to call Pusloski as a witness at a continuance of the suppression hearing.

The State does not dispute that two of the digital photos Pusloski reviewed during his search of the data files Apple provided in response to CDW-2 fall outside the warrant's date range. In his affidavit supporting the application for CDW-3, Pusloski represented the two digital photographs were of documents that bore dates outside CDW-2's authorized date range. Thus, the State concedes those photographs could not have existed during CDW-2's date range.

To fall under the plain view exception, "officer[s] must lawfully be in the area where [they] observed and seized the incriminating item or contraband, and it must be immediately apparent that the seized item is evidence of a crime." Gonzales, 227 N.J. at 101. The plain view exception is

applicable to searches of electronic data contained on computer devices, including devices that store digital data and images, including photographs. See, e.g., State v. Harris, 457 N.J. Super. 34, 45-47 (App. Div. 2018) (analyzing a search of data on "a CD provided in response to a CDW" under the plain view exception); U.S. v. Stabile, 633 F.3d 219, 236-37 (3d Cir. 2011) (addressing an officer's review of data files found on a computer hard drive folder under the plain view exception).

Here, the motion court rejected the State's reliance on the plain view exception based on its singular, conclusory factual finding that "law enforcement was not permitted to view photographs or material beyond what was permitted in CDW-2." The court otherwise relied on our decision in Harris, where we considered the applicability of the plain view exception to an officer's search of photographs on a "CD" supplied in response to a CDW, which did not authorize a search for photographs and otherwise limited the search to a defined date range. 457 N.J. Super. at 41-47. In Harris, the State argued the search and recovery of an incriminating photograph was covered by the plain view exception because the officer had a search warrant — the CDW — for the data on the CD, the officer inadvertently found the photograph

because he assumed it was within the authorized date range, and the photograph was immediately recognizable as evidence of a crime. Id. at 43.

We rejected the State's reliance on the plain view exception, reasoning the officer was not in a place he was authorized to be when he observed the photograph because the CDW did not authorize a search of the data for photographs. Id. at 46. More particularly, we determined "officer[s] [are] not in a lawful viewing place when [they] open[] JPEG files clearly containing photographs provided in a response to a CDW that does not authorize the review of photographs." Ibid.

We also found the search was not supported under the plain view exception because the photograph fell outside the authorized date range of the CDW. Id. at 47. That determination was based on a trial court factual finding that "[t]he folder date designations and the text files containing information regarding dates outside of the warrant further notified the police that the folders were not within the time frame of the warrant." Ibid. In other words, in Harris the electronic data folder designations and text files associated with the photograph made clear the data file containing the photograph was outside the CDW's authorized date range. Ibid.

Contrary to the motion court's determination here, the record does require or permit a finding that our holding in Harris compels suppression of the two photographs falling outside CDW-2's date range that Pusloski discovered during his search of the data. Our holding in Harris is founded in part on a fact not extant here; the CDW in Harris did not authorize a search for photographs, while CDW-2 expressly authorized Pusloski's search of photographs in the data Apple supplied. Ibid.

More importantly, in Harris we relied on a factual finding the "folder date designations and the text files containing information" associated with the photographs provided notice to the officer that the data folder in which the photograph was found was outside the date range of the CDW. Ibid. We are without a similar finding by the motion court. Nor could the motion court have made such a finding because there is no competent evidence any of the pertinent data files provided similar notice to Pusloski.[8]

Nonetheless, Harris teaches a determination as to whether the plain view exception applies to a search of digital evidence provided in response to a CDW requires a fact-sensitive analysis that is in part dependent on an

[8] In his certification submitted by the State as a supplement to the record on appeal, Pusloski states none of the "titles" to the "images" from defendant's "iCloud account" Apple produced in response to CDW-2 had "dates or times displayed."

understanding of the nature of the data and the pertinent digital technology. We recognized "the plain view doctrine applies to seizures of evidence during searches of computer files, but the exact boundaries of the doctrine will vary from case to case in a common-sense, fact-intensive matter." Id. at 46 (quoting Stabile, 633 F.3d at 240-41). Indeed, a court cannot properly analyze one of the essential elements of the plain view doctrine — whether an officer is "lawfully in the viewing area," Gonzales, 227 N.J. at 82 — without first determining and assessing the officer's location on the digital landscape presented by the data. Logic dictates that determination is dependent on the data presented, the pertinent digital technology, and a full understanding of the officer's actions comprising the search.

Here, the parties' dispute over whether the plain view exception applies to Pusloski's opening of the data files containing the two photographs outside CDW-2's date range centers on their conflicting claims over the digital characteristics of the data produced by Apple; Pusloski's available access to data, if any, permitting him to determine the relevant date of a data file to

assess whether the file was within the authorized date range; and Pusloski's actions in conducting the search.[9]

For example, defendant argued before the motion court, and argues again on appeal, Pusloski should have known the data files containing the two photographs were outside the authorized date range prior to opening them because: Apple's statement accompanying the data production warned that "certain data in the iCloud files" may not have been date filtered; Apple's

[9] The record is devoid of evidence defining the dates associated with a data file that were to be employed to determine whether a file falls within CDW's authorized date range. To be sure, a data file consisting of a digital photograph of a document bearing a date after the last date in CDW-2's authorized date range (e.g., a photograph of the front page of newspaper showing its date and describing incidents that occurred on the date) could not properly fall in the CDW-2 date range because the photograph could not have been taken during the authorized date range. On the other hand, a photograph of a newspaper dated before an authorized date range does not necessarily fall outside the permissible scope of a CDW because the photograph may be been on an electronic device, or transferred via the device, during the authorized date range. Although defendant argues the "creation" date reflected in the metadata associated with a data file that includes a digital photograph is dispositive of whether a file falls within CDW-2's date range, there is no record evidence supporting that interpretation of the data Pusloski received in response to CDW-2. Moreover, as we explain, the parties' dispute whether the "creation" date of a file, as reflected in the file's metadata, may be properly utilized to define the data file's date for purposes of determining whether the file falls within CDW-2's date range. We do not offer an opinion on these issues or suggest there are not many others relevant to a proper determination of the validity of Pusloski's opening of the data files containing the two photographs outside CDW's date range.

statement suggested Pusloski consult a cellular forensics expert before opening "certain data in the iCloud files"; and Pusloski did not confer with an expert prior to opening the files and observing the photographs. Defendant also argues that if Pusloski reviewed the metadata associated with the data files containing the photographs before opening them, it would have established the creation dates of the data files, thereby enabling the State to determine if the files were within CDW's authorized date range.

In contrast, the State argued before the motion court, and argues here, that metadata is unreliable, may be manipulated, and does not establish the date a photograph is actually first taken. The State also disputes defendant's claim that creation dates reflected in metadata establish the date relevant to determining whether a data file falls within CDW-2's date range. The State further contends that, unlike in Harris, there were no file names or other available data allowing Pusloski to determine whether the data files containing the photographs he observed were outside the date range without first opening the files and examining their contents. See Harris, 457 N.J. Super. at 47. Additionally, the State disputes defendant's version of the sequence and manner in which Pusloski reviewed the data files, and the State offered, and

offers, a version of Pusloski's review of the data files different than that claimed by defendant.

The court did not consider, address, or determine the parties' factual disputes over the manner in which Pusloski reviewed the files, the characteristics of the data files, and the digital and computer technology necessary to an understanding of Pusloski's search of the files. And the court did not engage in the requisite factual analysis to determine if Pusloski was in a place he was lawfully entitled to be when he viewed the two photographs outside CDW-2's date range such that it could properly determine if discovery of the photographs falls within the plain view exception. Instead, in circular fashion, without making any findings of fact, see R. 1:7-4, and without determining Pusloski's location on the digital landscape presented by the data and technology, the court concluded Pusloski was in a place he was lawfully entitled to be when he viewed the two photographs simply because the photographs are outside CDW-2's date range. For the reasons we have explained, the motion court's reliance on Harris to support that determination was in error.

Where, as here, there are disputed material issues of fact on a motion to suppress evidence, "testimony thereon shall be taken in open court." R. 3:5-

7(c). Moreover, where a dispute as to a material fact exists, "the trial court should not restrict the State or defendant in the presentation of all relevant evidence." State v. Randolph, 441 N.J. Super. 533, 554 (App. Div. 2015) (quoting State v. Hope, 85 N.J. Super. 551, 555 (App. Div. 1964)). Development of a record establishing the facts based on competent evidence is essential to proper fact findings by the motion court, and allows for proper appellate review, ibid., which is necessarily limited to the evidence presented at the suppression hearing, State v. Turcotte, 239 N.J. Super. 285, 299 (App. Div. 1990). Therefore, a motion court should afford the "parties the opportunity to probe the veracity of" disputed facts, State v. Parker, 459 N.J. Super. 26, 30-31 (App. Div. 2019), particularly where the legal issues presented are "exquisitely fact-sensitive and require the court's most discerning analysis," Randolph, 441 N.J. Super. at 555; see also State v. Aikens, 401 N.J. Super. 298, 309 (App. Div. 2008) ("the trial court should not have undertaken to decide the motion to suppress without hearing all the evidence" on a "complex" issue).

We recognize defendant and the State should have been more assertive in urging the court to conduct a full evidentiary hearing to resolve the numerous factual issues attendant to a proper determination of the issues

presented by defendant's motion, but the court should have nonetheless recognized the need for an evidentiary hearing to resolve the factual disputes, including the parties' dispute over the data, and what it showed and did not show, based on the pertinent technology. Although the court held a hearing, the testimony presented related solely to an issue — defendant's claim data extracted from his cellphone showed police attempted to search the phone without a warrant — unrelated to the propriety of Pusloski's search of the data produced by Apple in response to CDW-2. Thus, the court did not conduct an evidentiary hearing at all concerning Pusloski's search of the data from Apple.

We appreciate that prior to the hearing the DAG advised defense counsel the State did not believe an evidentiary hearing was necessary, but the State's mistaken assertion did not obviate the need for an evidentiary hearing to resolve the fact issues presented by the parties' conflicting versions of Pusloski's search of the data, as well as the data and the related technology. Indeed, defendant had the burden of presenting evidence supporting his challenge to Pusloski's search and seizure pursuant to CDW-2 but did not present any evidence at the hearing addressing the many factual issues raised in the parties' briefs and the arguments of counsel. See Keyes, 184 N.J. at 554.

The State belatedly recognized the court was confronted with fact issues necessary for a proper determination of the motion, and during the hearing it requested an opportunity to call Pusloski to testify at a later date concerning his search of the data and, presumably, the digital technology defining the landscape within which he reviewed the data and discovered the photographs. In our view, the court erred because it did not directly address the State's request but clearly rejected it by indicating in response that it would consider the arguments of counsel and then decide the motion. See Randolph, 441 N.J. Super. at 554; State v. Audette, 201 N.J. Super. 410, 414 (App. Div. 1985) (finding the motion court erred by failing to grant the State's motion to postpone a suppression hearing where the State failed to make arrangements for its law enforcement witness to attend).

Because the record revealed numerous fact issues pertinent to a proper disposition of the suppression motion, the court should not have decided the motion in the absence of an evidentiary hearing at which competent evidence was developed to support the findings necessary to support the court's determination. See R. 3:5-7(c) (requiring testimony to be taken in open court "if material facts are disputed"); see also State v. Burney, 471 N.J. Super. 297, 316-18 (App. Div. 2022) (remanding for new suppression hearing where

scientifically complex issue of fact required expert testimony); State v. Green, 346 N.J. Super. 87, 90-91 (App. Div. 2001) (explaining "an evidentiary hearing is required" where the parties' briefs submitted in accordance with Rule 3:5-7 "place[] material facts in dispute"). We therefore vacate the court's order and remand for the court to conduct an evidentiary hearing on defendant's suppression motion. R. 3:5-7(c); see also Green, 346 N.J. Super. at 90-91.

At the remand hearing, the parties shall be permitted to make any and all arguments pertinent to defendants' challenge to the validity of Pusloski's search of the data supplied by Apple in response to CDW-2, including any arguments made by defendant in support of his suppression motion that were previously rejected by the motion court in the absence of a fully developed evidentiary record. The State shall be permitted to produce evidence, including evidence beyond testimony from Pusloski, in support of its claims Pusloski's search of the data and discovery of the two photographs outside CDW-2's date range were within the proper scope of the warrant and, if not, the search was lawful under the plain view exception to the warrant

requirement.[10] The court shall conduct such proceedings as are required to allow the parties to present the evidence supporting their respective claims.

Our decision shall be not be construed as an expression of an opinion on the merits of the suppression motion. The court shall consider and decide the motion based on the competent evidence presented at the remand hearing. We note only that a determination of a motion to suppress evidence seized from a search of electronic data, with or without a warrant, presents unique and challenging issues. See, e.g., U.S. v. Richards, 659 F.3d 527, 539 (6th Cir. 2011) (citation omitted) (noting officers reviewing digital data may, "[a]s is the case with paper documents, on occasion in the course of a reasonable search, . . . examine, 'at least cursorily,' some 'innocuous documents . . . in order to determine whether they are, in fact, among those papers authorized to be seized,'" and collecting cases illustrating the "case-by-case" analysis of challenges to searches of digital data); Stabile, 633 F.3d at 241, n.16 (quoting United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1184 (9th Cir. 2010) (Callahan, J., concurring in part and dissenting in part)) (explaining "[a] measured approach based on the facts of the particular case is especially

[10] To the extent evidence presented at the remand hearing supports the State's claim the challenged evidence is admissible under the independent source exception to the warrant requirement, our decision does not preclude the State from renewing its argument the evidence is admissible on that basis.

warranted in the case of computer-related technology, which is constantly and quickly evolving."); People v. Hughes, 506 Mich. 512, 530-47 (Mich. 2020) (citation omitted) (discussing the numerous and complex legal issues implicated by a search of electronic data, including the permissible scope of a warrant for electronic data; explaining the propriety of an officer's "search of seized digital data" requires consideration of "whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant"; and detailing factors that should be considered in determining whether the search was reasonably directed at discovering evidence specified in a warrant).

We cite the foregoing cases as illustrative only. There are many others in the federal and state courts addressing the issues presented by searches of seized digital data. Our citation to the cases is not intended to define the legal principles upon which defendant's motion should be decided and does not constitute our adoption of any court's holdings or exposition of the correct legal principles. We cite the cases only because they confirm there are many issues in play when the evidence concerning Pusloski's search of the data provided by Apple is presented at the remand hearing. We leave it to the parties to raise whatever issues they deem appropriate based on the relevant

competent evidence presented, and to the remand court to make appropriate findings and legal conclusions in accordance with Rule 1:7-4.

Vacated and remand for further proceedings in accordance with this opinion. We do not retain jurisdiction.

I hereby certify that the foregoing is a true copy of the original on file in my office.

CLERK OF THE APPELLATE DIVISION