Filed 8/30/24

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

NATHANIEL DIMAGGIO, Petitioner, v. THE SUPERIOR COURT OF MONTEREY COUNTY, Respondent; THE PEOPLE, Real Party in Interest.	H051516 (Monterey County Super. Ct. No. 22CR004734)

Nathaniel DiMaggio brought this petition for writ of mandate (petition) to challenge the denial of a motion to suppress evidence obtained during a search of his cellphone and tablet. DiMaggio contends that, while the trial court correctly found the Monterey County Sheriff's Office (sheriff's office) exceeded the scope of the search warrant when executing the search, it erred in finding the sheriff's office acted in good faith and in denying the motion on that basis. On behalf of real party in interest the People, the Monterey County District Attorney claims the sheriff's office properly executed the search warrant and acted in good faith.

We agree with DiMaggio and will issue a peremptory writ of mandate directing respondent court to vacate its order denying DiMaggio's motion to suppress and to enter

a new order suppressing any evidence obtained by the sheriff's office falling outside the date and time limitations set forth in the search warrant.

I. FACTS AND PROCEDURAL BACKGROUND[1]

A. *Background, Search Warrant, and Charges*

Jane Doe accused DiMaggio of sexually assaulting her sometime during the evening of May 7, 2022,[2] into the morning of May 8, after they had drinks together at a restaurant with Jane Doe's husband and two of her friends.

Jane Doe called the sheriff's office on May 9 to report the sexual assault. With Jane Doe's permission, then-Detective Sergeant Brian Hoskins used Jane Doe's cellphone to conduct a pretext text exchange with DiMaggio to attempt to elicit an admission from DiMaggio that he sexually assaulted Jane Doe.

On May 16, Detective David Gonzalez, who was at that time assigned to the sexual assault and domestic violence unit, authored an affidavit and statement of probable cause (jointly, the affidavit) to secure a search warrant for DiMaggio's cellphone and tablet. In the statement of probable cause, Gonzalez set forth his training and experience. He stated that sexual assault perpetrators have been known to take photographs of their victims and store such images on their mobile devices.[3] He also observed that image and

---

[1] These facts are drawn from the evidence presented during the preliminary hearing on March 3, 2023, and during the hearing on DiMaggio's motion to suppress in September 2023.

[2] Unless otherwise indicated, all dates were in 2022.

[3] Detective Gonzalez included the following sentence in the statement of probable cause: "Furthermore, based on my training and experience that subjects who take sexual interest in minors will attempt to hide their activities on storage devices." That sentence is the only reference to minors in the statement of probable cause. Elsewhere, Gonzalez refers to the alleged sexual assault against Jane Doe, an adult: "I am expecting to find information that could link [DiMaggio] to this sexual assault." "By examining the text messages, videos, call logs, pictures, metadata, device location, it will assist investigators to establish a motive on why [DiMaggio] committed the sexual assault." At the hearing on the motion to suppress, Gonzalez testified that, at the time he drafted the search warrant, he had no reason to believe DiMaggio possessed child pornography.

video files "are often embedded with [metadata]," which can include the date and time the file was downloaded or created.[4] He cautioned that some image and video files "can have their creation times stripped out of their [metadata] which can make a date range not feasible." Relying on his training and experience, Detective Gonzalez asserted "that often within [*sic*] a device will have no date and time associated with data" and "that data will have incorrect dates and times associated with data." Thus, he requested in the statement of probable cause a search "for all content with a date and time or with no date and time associated to [*sic*] the data."

Detective Gonzalez drafted the proposed warrant to search DiMaggio's cellphone for categories of evidence, including images, related to the sexual assault of Jane Doe. Despite requesting a search for content with and without associated date and time information in the statement of probable cause, Gonzalez drafted the search warrant itself to authorize a search only for images falling within a one-month time period. Gonzalez did not include items without timestamps in the search warrant's exhibit (exhibit 1B) that listed items to be seized.

A judge of the Monterey County Superior Court found the warrant was supported by probable cause and issued search warrant 22SW000563 (search warrant).[5] As pertinent here, the search warrant authorized Monterey County peace officers to search DiMaggio's cellphone and tablet "for the following evidence, for the described time period: [¶] Time Period **[[Penal Code] § 1546.1[, subd.] (d)(1)[6]]**: **4.8.2022 at 0001 hours to 5.9.2022 at 2359 hours (Pacific Daylight Time)**[.] [¶] **Evidence:** All data constituting evidence and instrumentalities of sexual assaults including communications

---

[4] Samuel Plainfield testified during the hearing on the motion to suppress that metadata is data about data and noted that timestamps are a "standard" type of metadata, which typically indicate when the file was created, accessed, and modified.

[5] The parties stipulated to the existence of the search warrant and Detective Gonzalez's affidavit, set forth in People's exhibit No. 2, and DiMaggio's standing.

[6] Unspecified statutory references are to the Penal Code.

referring or relating to the above-listed criminal offenses, between from **4.8.2022 at 0001 hours to 5.9.2022 at 2359 hours (Pacific Daylight Time)** as follows: [¶] (1) All communications content, including email, text (short message service (SMS)/multimedia message service (MMS) or application chats), notes, or voicemail. This data will also include attachments, source and destination addresses, and time and date information, and connection logs, images and any other records that constitute evidence and instrumentalities of sexual assaults, including communications referring or relating to the above-listed criminal offenses, together with indicia of use, ownership, possession, or control of such communications or information found, including deleted data. [¶] . . . [¶] (3) All photographic/video/audio data and associated metadata, including deleted data." The date and time parameters appear in bold font in the search warrant.

As discussed in greater detail *post* (pt. I.B.), when the sheriff's office executed the search warrant, it found images of suspected child pornography on DiMaggio's cellphone. Detective Gonzalez then authored a second search warrant to search DiMaggio's cellphone, this time "for child pornography."[7]

The Monterey County District Attorney filed an information charging DiMaggio with numerous counts of sexual assault, including three counts of sexual assault of Jane Doe, and one count of possession of matter depicting a minor engaging in sexual conduct (§ 311.11, subd. (a); count 4).

B. *Motion to Suppress and Suppression Hearing*

DiMaggio filed a motion to suppress evidence obtained by the sheriff's office when they searched his cellphone and tablet pursuant to the first search warrant. The trial court treated DiMaggio's motion as three motions, one to quash, one to traverse the

[7] The second search warrant is not at issue in this petition.

search warrant, and one to suppress.[8] DiMaggio's motion to suppress requested the "suppression of 'any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution *or* [the California Electronic Communications Privacy Act (§ 1546 et seq.)],' " "including the fifteen images that form the basis of count four."

During the hearing on the motion to suppress in September 2023, witnesses described the process by which data on DiMaggio's cellphone and tablet was accessed, searched, and reviewed both by the sheriff's office and by DiMaggio's digital forensics expert witness.

Ryan Acevedo, a digital forensics investigator with the sheriff's office at the time of the execution of the search warrant in May 2022, extracted the data from DiMaggio's cellphone. On or about May 16, he received a copy of the search warrant and the exhibits attached thereto but not the statement of probable cause or any information about the case. He confirmed the date and time parameters on the search warrant before performing the extraction using a software program called GrayKey. After GrayKey extracted the data, Acevedo used a software program called Cellebrite Physical Analyzer to "unpack[] and parse[] out" the raw GrayKey data to present it in a readable format and filter the data to limit it to specific dates and times.[9]

Once the data was "unpacked" in Cellebrite, prior to generating the report, Acevedo checked the search warrant for the start and end dates of the temporal parameters, filtered the data for the timeframe indicated on the search warrant, and selected the option to include items that do not have any metadata. He explained that "[m]etadata is the information that is contained within a picture, and it has information on

---

[8] The trial court orally denied the motions to quash and to traverse the search warrant during a hearing on September 8, 2023, and later clarified those rulings in its order on the motion to suppress.

[9] Acevedo testified that Cellebrite was the only software available in May 2022 at the sheriff's office that he could use to read the GrayKey raw data.

it, [] such as where the picture was taken, the dates and times that it was taken," and later clarified that the option he selected in Cellebrite was "[i]tems without timestamps."

Acevedo explained that representatives from Cellebrite had trained him to check the "items without timestamps" box to "include all the data that you can get from the extraction into the report," even if the data was not within the search warrant parameters. Between February 2019 (when he first became certified to use the Cellebrite program) and May 2022, Acevedo estimated he conducted 200 to 300 extractions of electronically stored information using Cellebrite, including approximately 100 extractions that he performed pursuant to a search warrant. It was his "standard protocol" to include in the search results images that did not contain timestamps, even when performing extractions pursuant to a warrant, regardless of whether "items without timestamps" fell within the scope of the search warrant.

Cellebrite told him it was "best practice" to select the " 'items without timestamps' " option because it would allow the capture of data from which metadata had been scrubbed, and the attorneys or detectives would be responsible for determining whether the information fell within the search warrant parameters. He testified that he was "trained that the more information [he] captured in the limited Cellebrite reports, the more likely there would be detection of evidence of a crime," though it is not clear from the record who provided this guidance.

Acevedo followed this same practice when executing the search warrant on DiMaggio's cellphone. He applied a time filter for the dates indicated in exhibit 1B of the search warrant and selected the option to include items that did not have timestamps. He acknowledged that the enumerated types of evidence in exhibit 1B of the search warrant did not authorize a search for items without timestamps and that it was his job to use the parameters in the search warrant to generate the data report. However, he admitted that he does not typically read everything in the search warrant, and had not

read the list of evidence authorized for search and seizure in the search warrant prior to doing so during the hearing on the motion to suppress.

Acevedo provided the report containing the filtered data (limited report) to Detective Gonzalez. The data contained in the limited report should have had the same timestamps as the raw GrayKey data and the data in Cellebrite prior to generation of the report.

Before Detective Gonzalez began reviewing the limited report, he saw that it included data that fell within the temporal parameters of the search warrant as well as items without timestamps. Although he realized that the search warrant did not authorize a search for items without timestamps, he conducted an "[e]xtensive" search of the data in the limited report. While reviewing the limited report, he did not verify whether each image had a timestamp, but he noticed that there were items that did not have timestamps. He acknowledged that he "didn't pay too much attention to the date and time stamps. [He] was more looking for the pictures that were relevant to this investigation until [he] came across the photographs of the [child pornography]."

While reviewing the limited report, Detective Gonzalez found and documented "two or three images of suspected [child pornography]." He "eventually" found and documented additional images that he "concluded were consistent with alleged intent to possess [child pornography]." None of these images had any date or timestamps. Each of these images had a filename that ended with " 'embedded,' underscore, one dot, 'JPG.' "

Based on his review of the images in the limited report, Detective Gonzalez authored a second search warrant for DiMaggio's cellphone specifically targeting child pornography and requesting authorization to search for "data with no date or time stamps." Gonzalez eventually discovered the dates of the images of child pornography originally found during execution of the first search warrant after receiving the search results from the second search warrant. Based on the information from the second search

warrant, Gonzalez believed DiMaggio had received the images of child pornography between May 16, 2016, and October 15, 2020 (i.e., outside the date range set out in the search warrant).

Detective Sergeant Hoskins supervised Acevedo and Detective Gonzalez. He had trained Acevedo to read search warrants so that he would "know what parameters were to be searched," including identifying what items to seize and "looking at the date parameters of a warrant." Hoskins became aware that Acevedo used the filter option " 'items without time stamps' " when they found the first image of suspected child pornography in the limited report. In the course of reviewing the limited report, Hoskins saw other images, including other images of suspected child pornography, that did not have any metadata.

Samuel Plainfield, DiMaggio's digital forensics expert, reviewed the GrayKey raw data, the Cellebrite full data report, and the limited report. GrayKey stored the extraction of DiMaggio's cellphone data as a zip file. Plainfield used a software program called 7-Zip to open and view the raw GrayKey data.[10] In analyzing the GrayKey raw data extracted from DiMaggio's cellphone, Plainfield was able to find in the GrayKey raw data the file names for each of the images of suspected child pornography that formed the basis for Detective Gonzalez's second search warrant. He did so by searching for those file names in the limited report, which indicated the location of those files in the raw data. When he reviewed the images in question in the GrayKey raw data extraction, each

[10] Based on his review of these materials, Plainfield discovered that the Cellebrite full data report he received from the sheriff's office contained the images of suspected child pornography and also duplicate images that did not contain timestamp metadata; each of those images had filenames ending in "embedded_1." He testified that each image with a filename ending in "embedded_1" had been "stripped of their timestamp metadata." However, the "embedded_1" files did not appear in the GrayKey raw data. Plainfield also independently reviewed the GrayKey raw data using a separate Cellebrite Physical Analyzer—not the sheriff's office's copy of the Cellebrite Physical Analyzer—and found no "embedded_1" images.

contained timestamp metadata. He identified the timestamp metadata of these images, and found them to be timestamped prior to April 8, 2022.

After reviewing the parties' written closing arguments, the trial court denied DiMaggio's motion to suppress on October 17, 2023.[11] The court concluded that the evidence supported a finding that the sheriff's office's search of DiMaggio's cellphone had unlawfully exceeded the scope of the search warrant. However, the court decided the good faith exception to the exclusionary rule applied and concluded suppression of the evidence "would not [] deter future Fourth Amendment violations sufficiently to outweigh the costs" because "the evidence was seized as the result of an isolated software failure and use of an arguably justified filter by a no-longer-employed analyst."[12]

DiMaggio filed in this court a petition for writ of mandate contending the trial court erred in dismissing his motion to suppress based on the good faith exception to the exclusionary rule. This court issued an order to show cause and received further briefing from both parties.

II. DISCUSSION

DiMaggio contends the trial court erred by finding the sheriff's office acted in good faith when executing the search warrant and in denying his motion to suppress. He asserts that Acevedo knew as he was preparing the limited report, and Detective Gonzalez knew before reviewing it, that the information contained in the limited report exceeded the scope of the search warrant. Nevertheless, Acevedo proceeded to create the limited report, and Gonzalez conducted an extensive search of its contents.

The People counter that the sheriff's office's search did not exceed the scope of the search warrant because (1) the search warrant authorized the investigating officers

---

[11] The judge who ruled on the motion is the same bench officer who had previously signed the search warrant.

[12] Acevedo ceased working at the sheriff's office prior to the hearing on the motion to suppress.

" 'to access *all* data on the cellular device using electronic cellular telephone downloading equipment or device to determine if the data contains items described above,' " and (2) the search warrant does not use the term " 'timestamped.' " In the alternative, the People maintain that any sheriff's office actions that exceeded the scope of the search warrant were reasonable and "isolated" and do not call for exclusion of the challenged evidence.

A. *Legal Principles*

"A defendant may move to suppress evidence on the ground that a search or seizure with a warrant was unreasonable for various reasons." (*People v. Rowland* (2022) 82 Cal.App.5th 1099, 1109 (*Rowland*), citing § 1538.5, subd. (a)(1)(B)(i)–(v); see also § 1546.4, subd. (a).)

1. Search Warrants

"Both the United States Constitution and the Constitution and statutory law of California require that items seized pursuant to a search warrant be described with particularity." (*Bay v. Superior Court* (1992) 7 Cal.App.4th 1022, 1025 (*Bay*).)

The Fourth Amendment protects people from unlawful search and seizure. (U.S. Const., 4th Amend.) The California Constitution sets forth similar rights and requirements. (Cal. Const., art. I, § 13; see also § 1525.) The California Electronic Communications Privacy Act likewise requires, in pertinent part, that "[a]ny warrant for electronic information" (§ 1546.1, subd. (d)) "shall describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought."[13] (*Id*., subd. (d)(1).) "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As

[13] The exceptions to this requirement are not applicable here.

to what is to be taken, nothing is left to the discretion of the officer executing the warrant." (*Marron v. United States* (1927) 275 U.S. 192, 196 (*Marron*).) "The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." (*Maryland v. Garrison* (1987) 480 U.S. 79, 84 (*Garrison*).)

In furtherance of these protections, our courts have held "that in determining the property to be seized pursuant to a warrant, we are confined to the four corners of the warrant." (*Thompson v. Superior Court* (1977) 70 Cal.App.3d 101, 112 (*Thompson*).) The language of the search warrant "must be read in context and with common sense." (*People v. Eubanks* (2011) 53 Cal.4th 110, 134 (*Eubanks*).) Its scope should be " 'reviewed under an objective standard without regard to the subjective intent of the issuing magistrate or the officers who secured or executed the warrant.' " (*People v. Nguyen* (2017) 12 Cal.App.5th 574, 581 (*Nguyen*).) " 'Thus, the scope of the officer's authority *is determined from the face of the warrant and not from the affidavit*. The cogency of this rule becomes apparent when we consider the fact that the executing officer may not have a copy of the affidavit or even have knowledge of its contents when he serves the warrant.' " (*People v. MacAvoy* (1984) 162 Cal.App.3d 746, 756–757 (*MacAvoy*).) An affidavit may only be considered when interpreting the scope of a search warrant if (1) the warrant is deficient, (2) the affidavit is incorporated into the warrant by reference, and (3) the affidavit is attached to the warrant when law enforcement executes the warrant. (*Id*. at pp. 757–758.)

A search pursuant to "a valid warrant may nonetheless be unreasonable if the officers conducting the search exceed the scope of the warrant and, for example, begin looking for files that are not related to the subject of the search warrant." (*United States*

v. Johnston (9th Cir. 2015) 789 F.3d 934, 941 (*Johnston*).) Seizure of files and items beyond the scope of a search warrant for purposes of later review is " 'the kind of investigatory dragnet that the [F]ourth [A]mendment was designed to prevent.' " (*United States v. Tamura* (9th Cir. 1982) 694 F.2d 591, 595 (*Tamura*).) Once officers become aware that their search exceeds the scope of the search warrant, they must discontinue their search to the extent it contravenes the warrant's limitations. (See *Garrison*, *supra*, 480 U.S. at p. 87; *Nguyen*, *supra*, 12 Cal.App.5th at p. 584; see also *United States v. Loera* (10th Cir. 2019) 923 F.3d 907, 920 (*Loera*).)

2. The Exclusionary Rule and Good Faith Exception

"[T]he exclusionary rule generally bars admission of the evidence seized that was beyond the scope of the warrant." (*United States v. Sedaghaty* (9th Cir. 2013) 728 F.3d 885, 915 (*Sedaghaty*).) It is a "judicially created rule [that] is 'designed to safeguard Fourth Amendment rights generally through its deterrent effect' " (*Herring v. United States* (2009) 555 U.S. 135, 139–140 (*Herring*)) by "forbid[ding] the use of improperly obtained evidence at trial."[14] (*Id*. at p. 139; *People v. Willis* (2002) 28 Cal.4th 22, 30 (*Willis*).) The United States Supreme Court "has stressed that the 'prime purpose' of the exclusionary rule 'is to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures.' " (*Illinois v. Krull* (1987) 480 U.S. 340, 347 (*Krull*); see also *People v. Downing* (1995) 33 Cal.App.4th 1641, 1652.) By excluding evidence obtained through unlawful police conduct, " 'the courts hope to instill in those particular investigating officers, or in their future counterparts, a greater degree of care toward the rights of an accused.' " (*United States v. Leon* (1984) 468 U.S. 897, 919 (*Leon*).)

---

[14] Pursuant to the due process clause of the Fourteenth Amendment, the exclusionary rule also applies to the states. (*Mapp v. Ohio* (1961) 367 U.S. 643, 655; see also *Bay*, *supra*, 7 Cal.App.4th at p. 1025.)

An unconstitutionally unreasonable search does not necessarily trigger the application of the exclusionary rule. (*Herring*, *supra*, 555 U.S. at p. 140.) Courts must balance the deterrent and remedial effects against social costs. (*Krull*, *supra*, 480 U.S. at p. 347.) "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." (*Herring*, at p. 144; *People v. Leal* (2009) 178 Cal.App.4th 1051, 1065.)

The test is an objective one and "does not turn on the subjective good faith of individual officers" (*Krull*, at p. 355) or " 'the actual motivations of individual officers.' " (*People v. Sanders* (2003) 31 Cal.4th 318, 334 (*Sanders*).) Rather, the question is " 'whether a reasonably well trained officer would have known that the search was illegal' in light of 'all of the circumstances.' " (*Herring*, at p. 145; *Willis*, *supra*, 28 Cal.4th at p. 31.) "The requirement that the reasonableness of a search must be determined from the circumstances known to the officer when the search was conducted is consistent with the primary purpose of the exclusionary rule—to deter police misconduct. The rule serves ' "to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it." ' " (*Sanders*, at p. 334.)

The exclusionary rule does not apply if "an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and *acted within its scope*." (*Leon*, *supra*, 468 U.S. at p. 920, italics added.) The key to this good faith exception "is 'that the officers properly executed the warrant and *searched* only those places and for those objects that it was reasonable to believe were covered by the warrant.' " (*MacAvoy*, *supra*, 162 Cal.App.3d at p. 764.)

"[C]ourts must determine 'on a case-by-case basis' whether the circumstances of an invalid search pursuant to a warrant require the exclusionary rule's application." (*Willis*, *supra*, 28 Cal.4th at p. 32.)

3. Standard of Review

"In reviewing a trial court's ruling on a motion to suppress evidence, we defer to that court's factual findings, express or implied, if they are supported by substantial evidence." (*People v. Lenart* (2004) 32 Cal.4th 1107, 1119.) "We independently determine what legal principles are relevant, and apply those principles to the facts." (*People v. Aguilar* (1996) 48 Cal.App.4th 632, 637.) "We exercise our independent judgment in determining whether, on the facts presented, the search or seizure was reasonable under the Fourth Amendment." (*Lenart*, at p. 1119.) Likewise, " '[w]e review the trial court's application of the good faith exception de novo.' " (*Rowland*, *supra*, 82 Cal.App.5th at p. 1112.)

B. *Analysis*

The parties agree the search warrant at issue here was validly issued. The issues raised in this petition turn on the scope of the search warrant and the lawfulness of the subsequent search.

The plain language of the search warrant clearly limits the search authority to evidence falling within specific date and time parameters. Exhibit 1B of the search warrant sets forth (in bold font) the specific parameters of evidence authorized for seizure in both the section limiting the time period to be searched and again in the section that limits the type of data the officers may seize: "4.8.2022 at 0001 hours to 5.9.2022 at 2359 hours (Pacific Daylight Time)." (Boldface omitted.)

Detective Gonzalez described in the statement of probable cause the possibility that "some" photographs and videos could "have their creation times stripped out," which could "make a date range not feasible," and therefore requested to search for data with and without associated date and time information. However in the search warrant,

Gonzalez did not request authority to search for items without timestamps but instead requested data from a specific, one month time period.

Under the facts here, when assessing the constitutionality of the challenged search, we disregard the references in the probable cause affidavit to information without date and time information. "[W]e are confined to the four corners of the warrant" when "determining the property to be seized" (*Thompson*, *supra*, 70 Cal.App.3d at p. 112), and do not rely on the language of the affidavit where, as is the case here, the search warrant is not deficient. (*MacAvoy*, *supra*, 162 Cal.App.3d at pp. 757–758.) Further, we disagree with the dissent that the search warrant contains language incorporating the probable cause statement. (Dis. opn. of Manoukian, Acting P. J., *post*, at pp. 18–19.) The language cited by the dissent appears in the affidavit, not in the search warrant itself. The search warrant itself does not incorporate the affidavit or the statement of probable cause—it only incorporates exhibits 1A and 1B. Moreover, the affidavit did not accompany the search warrant when Acevedo executed the warrant. (*Ibid*.) Therefore, the search warrant authorized only the search for and seizure of data within the temporal limitations stated in the warrant. If Detective Gonzalez had wanted to search DiMaggio's cellphone and tablet for data that did not clearly fall within the date and time limitations, such as data without timestamps, he should have requested permission to do so in the search warrant itself.[15]

Nevertheless, the district attorney argues that the sheriff's office did not exceed the scope of the search warrant because it authorized the sheriff's office " 'to access *all* data' " on DiMaggio's cellphone. We reject this reading of the language in the search warrant. We agree with the trial court's legal conclusion that "[t]his language does not authorize law enforcement to *search* all data on the phone, rather, it acknowledges the

[15] Because he did not do so, we do not decide whether such a request would have satisfied the requirements of the Fourth Amendment. This decision would be for the issuing magistrate in the first instance.

technological reality that copying all data from the phone is a first and needed step that must be done prior to filtering the data for the items law enforcement may search." (Italics added.)

Furthermore, the reference to "all data" in exhibit 1B must be read and understood in context. (*Eubanks*, *supra*, 53 Cal.4th at p. 134.) The paragraph in exhibit 1B the district attorney references continues on to direct that "[t]hose items that are *within the scope of this warrant* may be copied and retained by investigative officers." (Italics added.) In addition, exhibit 1B states that the evidence the search warrant authorizes to be *searched* is "[a]ll data constituting evidence and instrumentalities of sexual assaults including communications referring or relating to the above-listed criminal offenses, between [] **4.8.2022 at 0001 hours to 5.9.2022 at 2359 hours (Pacific Daylight Time)**." The general language the district attorney relies on does not support the conclusion that the challenged evidence fell within the scope of the search warrant.

While the sheriff's office was authorized to *access* all the data on DiMaggio's cellphone and tablet, which they did by extracting the data using the GrayKey software, they were authorized to search for and seize only evidence of sexual assault falling within the timeframe specified in the search warrant. Acevedo knowingly exceeded the scope of the authorized search when he selected the option in the Cellebrite software to include in the limited report "[i]tems without timestamps" rather than limiting the search to the parameters of the search warrant. When Detective Gonzalez realized the limited report included items without timestamps and yet continued to conduct an "extensive" review, he, too, knowingly exceeded the scope of the search warrant. These decisions and actions occurred independently of any alleged Cellebrite software malfunction.

Contrary to the district attorney's contention, the absence of the term "timestamped" from the items listed in exhibit 1B of the search warrant does not render the search constitutional. An objectively reasonable officer would understand that date and time limitations in a search warrant for electronic information would require them to

filter the data in a manner that returned only items falling within that timeframe. Conversely, an objectively reasonable officer would not conclude that including items without timestamps would yield only items that comply with the temporal parameters of the search warrant. Rather, they would understand that such a search would be likely to yield both items that fall within the specified timeframe and items that fall outside of it.

Acevedo's testimony that he applied a date and time filter that matched the start and end dates specified in the search warrant indicates he understood the connection between the time limitation in the search warrant and the need to apply a filter based on timestamps. He acknowledged that his decision to also include items without timestamps was driven by his training, not by the terms of the search warrant. Likewise, Detective Gonzalez's testimony indicates a similar understanding. Neither witness provided any evidence that they would be able to determine, during the search of the cellphone, that any of the evidence that lacked a timestamp in fact fell within the search warrant's time limitation. For these reasons, substantial evidence in the record supports the trial court's finding that the search as conducted was "improper as outside the scope of the warrant."

With respect to application of the exclusionary rule, the district attorney contends the sheriff's office's search was reasonable because Acevedo selected the option "in Cellebrite that limited the time frame of the search" and Detective Gonzalez and Detective Sergeant Hoskins neither "began the search looking for pornography" nor "stop[ped] searching for responsive images after they found child pornography." In addition, they maintain that the actions in excess of the scope of the search warrant were "isolated" and not the product of systemic negligence.

"[W]hether a search is reasonable must be determined based upon the circumstances known to the officer when the search is conducted." (*Sanders*, *supra*, 31 Cal.4th at p. 334.)

In *Nguyen*, the search warrant authorized the search of " '[t]he residence located at: [address] described as a single story single family residence' " as well as " 'any and

all yards, garages, carports, outbuildings, storage areas and sheds assigned to the above-described premises.' " (*Nguyen*, *supra*, 12 Cal.App.5th at p. 578.) Law enforcement officers were aware that Nguyen lived in a separate residence behind the main family residence before searching his residence. (*Id*. at p. 579.) The Court of Appeal decided that Nguyen's residence could not reasonably be construed as being the family residence, a garage, an outbuilding, a storage area, or a shed. (*Id*. at p. 583.) Therefore, the court in *Nguyen* concluded officers lacked a good faith basis for searching Nguyen's residence because they knew before conducting the search that Nguyen's residence was not within the scope of the warrant. (*Id*. at p. 586.)

The situation here is similar to that faced by the officers in *Nguyen*. Acevedo knew the date and time restrictions of the search warrant. He testified that, consistent with his standard practice, he reviewed the search warrant for any date limitations and confirmed the specified dates before executing the search warrant by extracting and then filtering the data. Up to this point in the execution of the search warrant, we agree with the district attorney that Acevedo's actions were objectively reasonable. However, Acevedo's decision to also include in the limited report "[i]tems without timestamps" is unreasonable given his training from the sheriff's office on the law and practices applicable to search warrants for electronically stored information, which described the importance of any date parameters described in the search warrant. The record contains no evidence that would support a conclusion that the non-timestamped data would have fallen within the narrow date rate specified in the search warrant.

Acevedo testified that Cellebrite trained him to always select the "[i]tems without timestamps" option, regardless of whether the search warrant contained temporal limitations, in order to capture more data. He stated that it would be up to the detectives and attorneys to determine later whether the information fell within the scope of the search warrant. However, the objectively reasonable standard " ' "requires officers to have a reasonable knowledge of what the law prohibits" ' " (*Nguyen*, *supra*, 12

Cal.App.5th at pp. 586–587) and any " 'mistakes must be those of reasonable men, acting on facts leading sensibly to their conclusions of probability.' " (*Garrison*, *supra*, 480 U.S. at p. 87, fn. 11.)

Acevedo's decision to heed Cellebrite's advice to set time filters in accordance with the search warrant's temporal parameters but also select an option that includes items with no date-and-time-specific metadata is neither sensible nor compliant with well-settled law that, "in searches made pursuant to warrants only the specifically enumerated items may be seized." (*Tamura*, *supra*, 694 F.2d at p. 595; see also *Marron*, *supra*, 275 U.S. at p. 196 [the particularity requirement for search warrants "prevents the seizure of one thing under a warrant describing another"].) "[T]he wholesale *seizure* for later detailed examination of records not described in a warrant" (*Tamura*, *supra*, 694 F.2d at p. 595), as Acevedo stated Cellebrite trained him to do, "is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the [F]ourth [A]mendment was designed to prevent.' " (*Ibid.*) Acevedo's inclusion of items without timestamps in the limited report was not objectively reasonable.

At the time he reviewed the limited report produced by Acevedo, Detective Gonzalez, as the author of the affidavit and the search warrant, had specific knowledge of both the date and time parameters of the search warrant and of the dates of the claimed sexual assault of Jane Doe and of Detective Sergeant Hoskins' pretext messages with DiMaggio regarding the sexual assault. We infer from the fact that the temporal parameters of the search warrant end at "2359 hours" (boldface omitted) on May 9, the day after the timeframe of the alleged sexual assault and the day of the pretext communications between DiMaggio and Detective Sergeant Hoskins, that Detective Gonzalez particularly tailored such parameters to the sexual assault Jane Doe had described. (See *Garrison*, *supra*, 480 U.S. at p. 84.)

The district attorney cites *Loera* to support his position that the sheriff's office need not have ceased reviewing the limited report: "Although officers do not have to stop

executing a search warrant when they run across evidence outside the warrant's scope, they must nevertheless reasonably direct their search toward evidence specified in the warrant." (*Loera*, *supra*, 923 F.3d at p. 920.) But that did not occur here.

Detective Gonzalez acknowledged that, before he began reviewing the data in the limited report, he saw that it included items without timestamps.[16] Gonzalez testified that he knew that items without timestamps were not included in the scope of the search warrant, yet he proceeded to conduct an "[e]xtensive" search of the data in the limited report. (Cf. *Johnston*, *supra*, 789 F.3d at p. 942 [finding no further warrant required where the agent "was not digging around in unrelated files or locations that might have prompted the need for a second warrant"].) His actions, like Acevedo's, were not directed towards searching for the date and time-limited evidence specified in the search warrant and, thus, were not objectively reasonable under the circumstances.[17]

Once Detective Gonzalez became aware that the limited report included data outside the scope of the search warrant, he should have either requested Acevedo generate a new limited report that used only the date and time filters that complied with

---

[16] Detective Sergeant Hoskins similarly testified to also knowing that Acevedo used the filter " 'items without timestamps,' " but it is not clear from the motion to suppress hearing when Hoskins became aware of this.

[17] The dissent suggests that Detective Gonzalez could have "reasonably interpret[ed] the warrant" as permitting him to search for non-timestamped files (dis. opn. of Manoukian, Acting P. J., *post*, at pp. 21–23, 29–30). However, the record does not support the conclusion that he actually did so. Directly after the testimony quoted by the dissent (dis. opn. of Manoukian, Acting P. J., *post*, at p. 20), Detective Gonzalez testified that "[w]hen [he] saw the parameters of the search that had been conducted on [] Di[M]aggio's phone, and [he] saw the items without timestamps filter, [] [he] realize[d] that was not a provision that [he] had included in the search warrant," and he "knew it at that moment." Despite that realization, Gonzalez continued to conduct an "[e]xtensive" search. In addition, Detective Gonzalez sought and obtained a second search warrant to search for evidence of child pornography and specifically requested authorization to search for data "with no date or time stamps"—a request not included in the original search warrant. (Boldface omitted.) These facts show that Detective Gonzalez was aware of the limitations of the initial search warrant and that his search had exceeded those limitations.

the temporal limitations in the search warrant or authored a new search warrant that sought authority to search for items without timestamps. (See *Garrison*, *supra*, 480 U.S. at p. 87; *Sedaghaty*, *supra*, 728 F.3d at p. 914 ["To the extent the agents wanted to seize relevant information beyond the scope of the warrant, they should have sought a further warrant."]; *Nguyen*, *supra*, 12 Cal.App.5th at p. 584.) He was not entitled to do an "extensive search" of all the data in the limited report—including the data without timestamps.

The good faith exception to the exclusionary rule applies when law enforcement officers "confine their search in good faith to the objects of the warrant." (*United States v. Rettig* (9th Cir. 1978) 589 F.2d 418, 423; see also *Sedaghaty*, *supra*, 728 F.3d at pp. 914–915.) Because Acevedo, Gonzalez, and Hoskins did not act within the scope of the search warrant in conducting their search of DiMaggio's cellphone, but, rather, intentionally disregarded and substantially exceeded the limitations in the warrant's scope, the good faith exception does not apply.

The trial court concluded that the good faith exception was applicable in part because "the excesses in the search were the result of, at worst, an isolated negligent failure to detect a software malfunction. Had Cellebrite not malfunctioned, the images would have had timestamps, and would have been excluded from the limited report regardless of Acevedo's use of the 'items without timestamps' filter." However, even if the trial court were correct in its conclusion that Cellebrite malfunctioned,[18] Acevedo's

[18] Whether the Cellebrite software malfunctioned does not ultimately affect our conclusion in this appeal. Nonetheless, because the trial court relied on the alleged malfunction, we briefly describe it: The Cellebrite full and limited reports contained files without metadata (described in the record as duplicate "embedded_1" files), and the Cellebrite full report also contained the corresponding original images that did contain metadata. When DiMaggio's expert Plainfield examined the GrayKey raw data, he discovered that the original images of suspected child pornography in the GrayKey raw data contained timestamp metadata but the GrayKey raw data did not contain the duplicate "embedded_1" files that had been stripped of their metadata (see fn. 10, *ante*).

and Detective Gonzalez's actions in creating and reviewing the limited report would still have exceeded the scope of the search warrant. The Cellebrite malfunction did not cause the violation of DiMaggio's constitutional rights. Rather, it brought to light what appears to be the sheriff's office's deliberate practice of disregarding temporal parameters when executing search warrants for electronic information.

Acevedo stated that he included items that do not contain timestamps as part of his "standard protocol" for executing search warrants for electronically stored information, a protocol he used in approximately 100 extractions of such data from digital devices that he executed pursuant to a search warrant. Even though the record does not indicate how many of those extractions were conducted pursuant to a search warrant with temporal limitations, Acevedo testified that Cellebrite trained users of its software to include items without timestamps *regardless* of a search warrant's parameters.

Moreover, the misconduct was not limited to Acevedo. Detective Gonzalez, too, reviewed the limited report and conducted further investigation based on it, even as he realized that evidence contained in the report was not limited to the date and time parameters set out in the search warrant. Thus, both Acevedo and Gonzalez independently violated DiMaggio's rights under the Fourth Amendment. We do not agree with the trial court that Acevedo's discontinued employment with the sheriff's office supports a conclusion that exclusion of the evidence unlawfully searched would be of little deterrent effect.

Based on the evidence elicited at the hearing on the motion to suppress, the sheriff's office's actions in executing the search warrant were not a mere one-time or intermittent " 'blunder[]' " by law enforcement (*Herring*, *supra*, 555 U.S. at p. 148), but,

---

Plainfield surmised that the Cellebrite software was responsible for generating the duplicate files. By selecting the Cellebrite filters he did, Acevedo's limited report excluded the timestamped original images, but included the duplicate files (which were not timestamped).

rather, were part of its "standard protocol" and, thus, evidence "systemic error or reckless disregard of constitutional requirements." (*Id*. at p. 147.) Moreover, the record does not suggest that the sheriff's office's actions were "motivated by considerations of practicality rather than by a desire to engage in indiscriminate 'fishing.' " (*Tamura*, *supra*, 694 F.2d at p. 597.) Indeed, Acevedo stated that he was "trained that the more information [he] captured in the limited Cellebrite reports, the more likely there would be detection of evidence of a crime." Even without Acevedo's admission, the United States Supreme Court has "historically recognized that the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.' " (*Riley v. California* (2014) 573 U.S. 373, 401.)

We conclude that the sheriff's office's conduct was sufficiently purposeful and culpable that exclusion of the evidence obtained by the sheriff's office in excess of the scope of the search warrant can meaningfully deter future unlawful conduct (*Herring*, *supra*, 555 U.S. at p. 144; *Krull*, *supra*, 480 U.S. at p. 347), either " 'in those particular investigating officers, or in their future counterparts.' " (*Leon*, *supra*, 468 U.S. at p. 919.) At oral argument in this matter, DiMaggio clarified that he seeks exclusion only of that evidence seized pursuant to the search warrant falling outside of the date and time limitations listed in the warrant. We decide exclusion of such evidence is warranted.

III. DISPOSITION

Let a peremptory writ of mandate issue directing respondent court to vacate its October 17, 2023 order denying petitioner's motion to suppress on the basis of the good faith exception to the exclusionary rule and to enter a new order granting the motion to suppress as to evidence obtained by the sheriff's office that falls outside the date and time limitations listed in search warrant 22SW000563. Upon issuance of the remittitur, this court's stay order is vacated.

_____
Danner, J.

I CONCUR:

_____
Lie, J.

BAMATTRE-MANOUKIAN, ACTING P. J., Dissenting.

I respectfully dissent from the majority's conclusion that the good faith exception to the exclusionary rule does not apply on the facts of this case. In its thorough ruling, the trial court made extensive findings of fact supported by substantial evidence. This court is required to give these factual findings deference while exercising our independent judgment to determine if the good faith exception applies. The trial court's factual finding that law enforcement "acted in objective good faith and reliance on the search warrant and affidavit" supports an independent determination that the good faith exception applies, even assuming that the scope of the warrant was exceeded. Within the context of the historical facts determined by the trial court, I agree with the trial court that application of the exclusionary rule to evidence with no timestamp metadata—including the images of suspected child pornography—is not warranted on the facts of this case.

I. FACTUAL AND PROCEDURAL BACKGROUND

I include a factual and procedural summary here to provide the basis for the trial court's factual findings.

A. The Warrant and Probable Cause Statement

Detective David Gonzalez, a Deputy Sheriff with the Monterey County Sheriff's Office, authored the probable cause statement in support of the warrant application in this matter. The affidavit detailed an alleged sexual assault by petitioner on the night of May 7–8, 2022. The probable cause statement reported that an acquaintance of petitioner alleged that petitioner committed sexual acts upon her after she consumed alcohol and fell asleep. Gonzalez's probable cause statement also stated that the alleged victim reported that she exchanged text messages with petitioner the next day about the alleged sexual assault. The probable cause statement stated that a search of petitioner's vehicle discovered a cell phone that petitioner indicated belonged to him, along with an iPad. Gonzalez's probable cause statement stated that he expected to find various types of files

on petitioner's phone relevant to the sexual assault investigation, including text messages, photos, and videos.

The probable cause statement stated Gonzalez's knowledge about the capabilities of modern cell phones based on his experience and training, including that images and videos on cell phones are often embedded with metadata that provides additional information about such files. Gonzalez stated that the information in metadata "can be but is not limited to creation date and time" and "can show when an image was downloaded/created." The probable cause statement also averred: "It should also be noted that some photographs and or videos can have their creation times stripped out of their METADATA which can make a date range not feasible." Thus, the probable cause statement set forth: "I am requesting the electronic storage devices be searched for all content with a date and time or with no date and time associated to the data. Based on my training and experience and in speaking with forensic examiners of cell phone devices, I know that often within a device will have [*sic*] no date and time associated with data. I also know that data will have incorrect dates and times associated with data. For these reasons, as well as due to the serious nature of the crimes being investigated, I am requesting all content from the device with all date/time and/or no date/time."

The resulting warrant listed the "Place(s)/Device(s) to be searched" as petitioner's phone and tablet, with no further restrictions as to what parts of the phone and tablet could be searched. As to the "Evidence to be seized," the warrant authorized law enforcement to search the cell phone for "[a]ll data constituting evidence and instrumentalities of sexual assaults including communications referring or relating to the above-listed criminal offenses, between from **4.8.2022 at 0001 hours to 5.9.2022 at 2359 hours (Pacific Daylight Time)**."

The sheriff's office then executed the warrant and found images of suspected child pornography on petitioner's phone. Gonzalez then obtained a second search warrant authorizing the sheriff's office to search the "[e]ntire contents of [the] phone to include

data with no date or time stamps" for "[a]ll data constituting evidence and instrumentalities of sexual assaults and possession of child pornography . . . ." The Monterey County District Attorney's Office filed an information that charged petitioner with various sexual offenses and other offenses, including one count of possession of matter depicting a minor engaging in sexual conduct (Pen. Code, § 311.11, subd. (a); count 4).

B. Motion to Suppress

Petitioner moved to suppress evidence of suspected child pornography found on his cell phone. Ryan Acevedo, a digital forensics investigator with the sheriff's office, testified that when he would examine a cell phone pursuant to a warrant, he would only receive the warrant, not the probable cause statement or any other information about the case. Acevedo testified that he extracted the data from petitioner's phone using a program called GrayKey that extracts all information from the phone, and that at this step, there is no option to select date and time filters. He also testified that there is no way to manipulate the data, including changing metadata, as it is extracted using GrayKey. Acevedo testified that he then used the Cellebrite software program, which "unpacks and parses out the data that was captured through the GrayKey and presents it into a readable layout." Acevedo testified that he could not and did not change any metadata at this stage. Acevedo testified that he applied filters to list files with timestamps within the date and time period listed in the search warrant while creating the Cellebrite report. He testified that he also checked a box that would include files with no metadata in the Cellebrite report. Acevedo testified that it was his "standard protocol" to include images with no metadata when generating a Cellebrite report. Cellebrite generated a report containing the filtered data, which Acevedo provided to Gonzalez.

Gonzalez testified that he provided Acevedo with a copy of the search warrant; he did not testify that he provided Acevedo with the probable cause statement. Gonzalez testified that it is common in cases he investigated to look for images that do not contain

metadata, stating: "Sometimes the metadata is not transferred from a -- say, when it's uploaded, it won't get uploaded with the metadata. Or, if you send it as a text message, it won't get -- sometimes, if you have the function selected to withdraw the metadata, that could be a reason." Gonzalez testified that he was not aware that Acevedo selected the option to include files with no metadata in the Cellebrite report. Gonzalez testified that when he reviewed the Cellebrite report, he saw that it included items without timestamps. Petitioner's counsel then asked Gonzalez, "When you saw items without timestamps, did you realize that wasn't in the warrant you had obtained?" Gonzalez replied, "It was in the statement of probable cause." When petitioner's counsel questioned further, Gonzalez replied that he knew at the moment he saw the items without a timestamp in the Cellebrite report that the warrant did not specifically state that non-timestamped files could be searched, and that he nonetheless conducted an "[e]xtensive search" of the files in the Cellebrite report.

Asked if he noticed whether some of the 169,113 images in the Cellebrite report had timestamps inside the date and time range listed in the warrant, Gonzalez testified, "I'm assuming the dates were -- I mean, the images were date-stamped . . . in some sort of way." Defense counsel asked Gonzalez whether he was aware "that 70 percent of the images on Mr. Di[M]aggio's phone were included in" the Cellebrite report; Gonzalez replied that he did not know. Gonzalez testified that as he reviewed the images in the Cellebrite report, he did not check to see if each image did or did not have a timestamp. Gonzalez testified that he continued to review the images in the report after discovering the first image of suspected child pornography. Gonzalez testified that he did not believe that any of the 15 images of suspected child pornography he found contained date or time metadata. He testified that based on the images of suspected child pornography he observed in the Cellebrite report, he sought and obtained a second search warrant for the same phone specific to items of child pornography. This second warrant authorized law enforcement to search the "[e]ntire contents of [the] phone to include data with no date or

time stamps" for evidence of sexual assault and possession of child pornography. Gonzalez testified that he did not learn the dates associated with the images of suspected child pornography until after he obtained the results of the second search warrant.

Gonzalez also testified that as he reviewed the 169,000-plus images in the Cellebrite report, it did not occur to him that the number of images might represent more than one month's worth of images, and he testified: "I didn't pay too much attention to the date and time stamps. I was more looking for the pictures that were relevant to this investigation until I came across the photographs of the [child pornography]." Gonzalez testified that he believed the Cellebrite report in this matter contained the "largest" number of images he had seen for a one-month period, but that "it's not abnormal to have that many images" because a Cellebrite report will include not only pictures but also emojis and icons. He also testified that he found one video relevant to the investigation into petitioner's alleged sexual assault in reviewing the Cellebrite report. Gonzalez's search also revealed the pretext conversation text messages between the alleged victim's phone and petitioner regarding the alleged sexual assault.

Sergeant Bryan Hoskins, a detective sergeant for the Monterey County Sheriff's Office, testified that he oversaw the investigation in this case from May to October 2022. Hoskins testified that he trained Acevedo to look at the date parameters of a warrant. However, Hoskins testified that he did not direct Acevedo in the instant search, as by this point Acevedo "was doing extractions pretty well on his own." Hoskins testified that he learned that Acevedo selected the option in Cellebrite to include files with no metadata when "one of the first images" of child pornography was located on the phone without metadata. Hoskins testified that he reviewed the images in the Cellebrite report along with Gonzalez and that he saw images of suspected child pornography without metadata. Hoskins testified that he did not discuss the lack of metadata on images with Gonzalez and that the embedded_1 file names for the images of suspected child pornography did not have any significance to him.

Samuel Plainfield, a forensic investigator, testified for petitioner as an expert in digital forensic investigations.[19] Plainfield testified that he analyzed the GrayKey raw data extracted from petitioner's phone, that he was able to identify the timestamp metadata associated with the 15 images of suspected child pornography in the raw data, and that this metadata showed these images were dated before April 8, 2022, the start date of the timeframe specified in the warrant. Plainfield testified that the full Cellebrite report, when compared to the GrayKey raw data, "contains an additional file with the moniker, underscore embedded_1 at the end of it, and that particular file has the metadata stripped off of it." Plainfield testified that Cellebrite "must have" created these embedded_1 images "because if it's not in the raw data and it appears somewhere else, the inference is that Cellebrite must have fabricated that." Plainfield testified that of the estimated 169,000 images in the Cellebrite report, "something like 90 percent" of those images were embedded_1 images stripped of their metadata, meaning that "90 percent of the images on the limited [Cellebrite] report were not in the raw data of Mr. Di[M]aggio's phone." Plainfield was then asked whether he had ever seen Cellebrite create a duplicate of an image and then strip it of its metadata. Plainfield responded as follows: "I had never observed that specific behavior, no. . . . I mean, it comes up right away that there's no timestamps in most of the pictures, and I find that to be odd, and I would look further into that." On cross-examination, Plainfield agreed that "Cellebrite somehow created or fabricated images ¶. . . ¶ [a]nd metadata." Plainfield also agreed that he had "never observed this kind of file re-creation or fabrication by Cellebrite before," and he testified that it "appears" that Cellebrite created or fabricated the embedded_1 files in this matter. Plainfield also testified on cross-examination that he did not believe it is possible for someone using Cellebrite to manipulate the information

[19] Hoskins and Acevedo also testified for the defense; it is not necessary to summarize their testimony for the defense here.

being loaded into the program and thus Cellebrite, not any user of the program, created or fabricated the embedded_1 images in this matter.[20]

C. Trial Court's Ruling

The trial court denied petitioner's motion to suppress in a written ruling. The trial court first concluded that the search of petitioner's phone exceeded the scope of the warrant and that the probable cause affidavit could not be used to affect the scope of the warrant. As to how the embedded_1 files with no metadata were created and included in the Cellebrite report, the trial court stated that "it is clear that something went wrong," and that "[w]hether it was a software glitch or user error," the embedded_1 images with no metadata were created. The trial court noted Plainfield's testimony that the Cellebrite software "must have" created the embedded_1 images and it stated that Plainfield "had not previously seen the creation or duplication of images by Cellebrite." The trial court also recounted Plainfield's testimony that Acevedo "did not create or fabricate the images," and the trial court concluded: "No evidence was presented to support a determination that the creation or duplication of images had previously resulted from Acevedo's extraction process."

The trial court then concluded that the good faith exception to the exclusionary rule applied. The trial court cited Gonzalez's probable cause statement in concluding: "[I]t does not appear that the government engaged in the type of 'deliberate overreaching' that has been held to be impermissible. [Citation.] Rather, as the evidence confirmed that date and time stamps may be modified by, *inter alia*, operating system updates and that images may be scrubbed of metadata, it appears that [the sheriff's office] in their extraction and search were 'motivated by considerations of practicality rather than by a desire to engage in indiscriminate fishing.' [Citation.]" The trial court stated: "Here, it

[20] A forensic investigator with the Monterey County District Attorney's Office testified as an expert in digital forensics in rebuttal of Plainfield's testimony. It is not necessary to summarize this witness's testimony here.

appears that the excesses in the search were the result of, at worst, an isolated negligent failure to detect a software malfunction. Had Cellebrite not malfunctioned, the images would have had timestamps, and would have been excluded from the limited report regardless of Acevedo's use of the 'items without timestamps' filter. There was no evidence that Cellebrite routinely malfunctioned in such a manner, or had ever previously so malfunctioned." The court further stated: "Acevedo's use of the 'items without timestamps' filter may not have been authorized by the warrant, but testimony concerning the existence of images with scrubbed metadata was proffered to explain its use. Acevedo relied on his Cellebrite training and understanding of the warrant in using the filter . . . ." In this situation, the trial court stated that it saw "little, if any, deterrent benefit to excluding evidence when the evidence was seized as the result of an isolated software failure and use of an arguably justified filter by a no-longer-employed analyst."

II. LEGAL PRINCIPLES AND STANDARD OF REVIEW

The Fourth Amendment to the United States Constitution provides that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." (U.S. Const., 4th Amend.) The goal of this particularity requirement is " 'to prevent general searches.' " (*People v. Amador* (2000) 24 Cal.4th 387, 392.) " 'By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.' [Citation.]" (*Ibid.*) "There is probable cause for a search if 'there is a fair probability that . . . evidence of a crime will be found in a particular place.' [Citation.] The probable cause showing must be made in the warrant affidavit [citation] and, as noted, the scope of the search must be 'no broader than the probable cause on which [the warrant] is based.' [Citations.]" (*Price v. Superior Court* (2023) 93 Cal.App.5th 13, 35–36.)

In reviewing whether a warrant states with sufficient particularity the place to be searched and the persons or things to be seized, courts generally examine whether the warrant stated the specific crime(s) being investigated. (See, e.g., *United States v. Palms* (10th Cir. 2021) 21 F.4th 689, 700 (*Palms*) ["warrant's limitation to evidence of the crime of human trafficking satisfied the Fourth Amendment's particularity requirement. [Fn. omitted.]"]; *United States v. Cobb* (4th Cir. 2020) 970 F.3d 319, 329 (*Cobb*) [" 'a warrant may satisfy the particularity requirement *either* by identifying the items to be seized by reference to a suspected criminal offense *or* by describing them in a manner that allows an executing officer to know precisely what he [or she] has been authorized to search for and seize.' [Citation.] The warrant need not satisfy *both* criteria. [Citation.]"]; *United States v. Castro* (6th Cir. 2018) 881 F.3d 961, 965 (*Castro*) ["A warrant that empowers police to search for something satisfies the particularity requirement if its text constrains the search to evidence of a specific crime. [Citations.]"].) Thus, in *United States v. Hall* (7th Cir. 1998) 142 F.3d 988 (*Hall*), the reviewing court held that warrants that authorized law enforcement to search computer media "which may be, or are used to visually depict child pornography, child erotica, information pertaining to the sexual interest in child pornography, sexual activity with children or the distribution, possession or receipt of child pornography, child erotica or information pertaining to an interest in child pornography or child erotica . . . computerized or other materials and photographs depicting sexual conduct, whether between adults or between adults and minors" were not prohibited general warrants. (*Id.* at pp. 995–996.) The court held that "the search warrants were written with sufficient particularity because the items listed on the warrants were qualified by phrases that emphasized that the items sought were those related to child pornography," and thus, "[p]olice officers executing the warrants were not unguided and free to rummage through Hall's property." (*Id.* at pp. 996–997, fn. omitted.)

"Exclusion of evidence due to a Fourth Amendment violation is not automatic." (*People v. Macabeo* (2016) 1 Cal.5th 1206, 1219 (*Macabeo*).) "The exclusionary rule applies only 'where its deterrence benefits outweigh its "substantial social costs." ' [Citations.]" (*People v. Robinson* (2010) 47 Cal.4th 1104, 1124.) "Suppression of evidence . . . has always been our last resort, not our first impulse. . . . We have rejected '[i]ndiscriminate application' of the rule, [citation], and have held it to be applicable only 'where its remedial objectives are thought most efficaciously served,' [citation] --that is, 'where its deterrence benefits outweigh its "substantial social costs," ' [citations]." (*Hudson v. Michigan* (2006) 547 U.S. 586, 591 (*Hudson*).)

"The good faith exception to the exclusionary rule applies when police act in objectively reasonable reliance on a search warrant issued by a detached and neutral magistrate. [Citation.] The prosecution bears the burden to prove officers' reliance on a warrant was objectively reasonable. [Citation.] 'This objective standard "requires officers to have a reasonable knowledge of what the law prohibits." ' [Citations.]" (*People v. Nguyen* (2017) 12 Cal.App.5th 574, 586–587 (*Nguyen*).) "Under the good faith exception to the exclusionary rule, evidence will not be suppressed if the police officer had an objectively reasonable belief the search or seizure was constitutionally permissible. [Citations.]" (*People v. Pearl* (2009) 172 Cal.App.4th 1280, 1292.) "Accordingly, our good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." (*United States v. Leon* (1984) 468 U.S. 897, 922, fn. 23 (*Leon*).) Where "the prosecution invokes the good faith exception, the government has 'the burden . . . to prove that exclusion of the evidence is not necessary because of [that] exception.' [Citation.] Thus, 'the government has the burden of establishing "objectively reasonable" reliance' under *Leon*. [Citation.] Establishing that the source of the error acted objectively reasonably is part of that burden. [Citations.]" (*People v. Willis* (2002) 28 Cal.4th 22, 36–37 (*Willis*).)

Courts applying the good faith exception have utilized four principles relevant to the analysis in the instant case.

A. The Reviewing Court Relies on a Trial Court's Findings of Fact That Are Supported by Substantial Evidence.

First, a reviewing court relies on a trial court's factual findings in determining whether the good faith exception applies. In reviewing a trial court's decision to grant or deny a motion to suppress evidence, "we rely on the trial court's express and implied factual findings, provided they are supported by substantial evidence, to independently determine whether the search was constitutional. [Citation.] 'Thus, while we ultimately exercise our independent judgment to determine the constitutional propriety of a search or seizure, we do so within the context of historical facts determined by the trial court.' [Citation.] It is the trial court's role to evaluate witness credibility, resolve conflicts in the testimony, weigh the evidence, and draw factual inferences. [Citation.] We review those factual findings under the deferential substantial evidence standard, considering the evidence in the light most favorable to the trial court's order. [Citation.]" (*People v. Moore* (2021) 64 Cal.App.5th 291, 296–297 (*Moore*).)

B. Even if Law Enforcement Exceeds the Scope of the Warrant, the Good Faith Exception Applies if Law Enforcement Had an Objectively Reasonable Belief that the Search Was Authorized by a Valid Warrant.

Second, the mere fact that law enforcement exceeds the limits of a warrant does not automatically preclude application of the good faith exception. The majority cites *United States v. Rettig* (9th Cir. 1978) 589 F.2d 418, 423 (*Rettig*) in concluding that "[b]ecause Acevedo, Gonzalez, and Hoskins did not act within the scope of the search warrant in conducting their search of DiMaggio's cellphone, but, rather, intentionally disregarded and substantially exceeded the limitations in the warrant's scope, the good faith exception does not apply." (Maj. opn. *ante*, at p. 21.) However, *Rettig* did not state that a search must strictly adhere to the scope of the warrant for the good faith exception

to apply. Instead, *Rettig* cited a Fifth Circuit case for the proposition that " '(t)he search must be one directed in good faith toward the objects specified in the warrant or for other means and instrumentalities by which the crime charged had been committed. It must not be a general exploratory search . . .' [Citations.]" (*Rettig*, *supra*, at p. 423.) Thus, the court in *Rettig* held that because "the agents did not confine their search in good faith to the objects of the warrant, and that while purporting to execute it, they substantially exceeded any reasonable interpretation of its provisions," suppression of evidence was required. (*Ibid.*) *Rettig* thus demonstrates that the good faith exception can apply where law enforcement exceeds the strict limits of the warrant, so long as law enforcement reasonably interpreted the provisions of the warrant and did not expand the search into a general exploratory search. Courts have similarly recognized that the good faith exception can apply when law enforcement exceeds the scope of the warrant, so long as law enforcement had an objectively reasonable belief that the search was within the warrant's limits. (See, e.g., *Leon*, *supra*, 468 U.S. at p. 918, fn. 19 [the good faith exception "assumes, of course, that the officers properly executed the warrant and searched only those places and for those objects that it was reasonable to believe were covered by the warrant"]; *People v. Meza* (2023) 90 Cal.App.5th 520, 544 ["officers may not rely on the good faith exception when they have knowingly exceeded the scope of a warrant"].) The "basic inquiry" in determining whether the good faith exception applies is whether "the officers had a good faith objectively reasonable belief that the *search they conducted* was authorized by a valid warrant. What is important is 'that the officers properly executed the warrant and *searched* only those places and for those objects that it was reasonable to believe were covered by the warrant.' [Citation.] This is the essential prerequisite to the reasonable good faith exception." (*People v. MacAvoy* (1984) 162 Cal.App.3d 746, 764.)

C. The Exclusionary Rule Requires Weighing the Likely Deterrent Effect Achieved by Suppressing the Evidence Against the Costs of Suppressing the Evidence.

Third, in applying the exclusionary rule, the United States Supreme Court "has examined whether the rule's deterrent effect will be achieved, and has weighed the likelihood of such deterrence against the costs of withholding reliable information from the truth-seeking process. [Citations.]" (*Illinois v. Krull* (1987) 480 U.S. 340, 347–348 (*Krull*).) "As with any remedial device, application of the exclusionary rule properly has been restricted to those situations in which its remedial purpose is effectively advanced." (*Id*. at p. 347.) Thus, suppression of evidence is not appropriate where "the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion." (*Leon*, *supra*, 468 U.S. at p. 922.) "The high court has also applied the good faith exception when officers have acted in reasonable reliance on information that subsequently is determined to be inaccurate. These cases, too, emphasize the deterrence rationale." (*Macabeo*, *supra*, 1 Cal.5th at p. 1222.)

D. Suppression of Evidence is Not Warranted Because of Mere Negligence or Error by Law Enforcement.

Fourth and finally, mere negligence or error by law enforcement does not preclude application of the good faith exception. "*Leon* teaches that the exclusionary rule should not be applied where exclusion cannot be expected to serve ' "as an incentive for the law enforcement profession *as a whole* to conduct themselves in accord with the Fourth Amendment." [Citations.]' [Citation.]" (*Willis*, *supra*, 28 Cal.4th at p. 48.) Thus, "the good faith exception does not apply where law enforcement is collectively at fault for an inaccurate record that results in an unconstitutional search. [Citations.]" (*Id*. at p. 49.) "[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." (*Herring v. United States* (2009) 555 U.S. 135, 144 (*Herring*).) Conversely: "[W]hen police mistakes are the

result of negligence . . . rather than systematic error or reckless disregard of constitutional requirements, any marginal deterrence does not 'pay its way.' [Citation.]" (*Id.* at p. 147.)

III. ANALYSIS

Applying the principles outlined above to the record before this court, I would hold that the good faith exception applies. Within the context of the historical facts determined by the trial court—factual findings that are supported under the deferential substantial evidence standard of review—my independent judgment is that the "last resort" of suppressing all evidence containing no timestamp metadata from petitioner's phone is not warranted on the facts of this case. (*Hudson*, *supra*, 547 U.S. at p. 591.)

A. The Trial Court's Findings of Fact Are Supported by Substantial Evidence.

First, the trial court's findings of fact are supported by substantial evidence and support the conclusion that the good faith exception applies. In its thorough ruling, the trial court made several findings of fact, including that: "it is clear that something went wrong" in the extraction of petitioner's phone; "[n]o evidence was presented to support a determination that the creation or duplication of images had previously resulted from Acevedo's extraction process"; because "the evidence confirmed that date and time stamps may be modified by, *inter alia*, operating system updates and that images may be scrubbed of metadata, it appears that [sheriff's officials] in their extraction and search were 'motivated by considerations of practicality rather than by a desire to engage in indiscriminate fishing.' [Citation.]"; "it appears that the excesses in the search were the result of, at worst, an isolated negligent failure to detect a software malfunction"; "[t]here was no evidence that Cellebrite routinely malfunctioned in such a manner, or had ever previously so malfunctioned"; the trial court saw "little, if any, deterrent benefit to excluding evidence when the evidence was seized as the result of an isolated software failure and use of an arguably justified filter by a no-longer employed analyst"; and

application of the exclusionary rule was not warranted in part because "it appears that [sheriff's officials] acted in objective good faith and reliance on the search warrant and affidavit, and their understanding of how Cellebrite functioned, and that exclusion of the evidence would not sufficiently deter future Fourth Amendment violations sufficiently to outweigh the costs."

Substantial evidence supports the trial court's factual findings. The trial court's findings regarding the cause of the creation of the embedded_1 files with no metadata were supported by reference to Plainfield's testimony. No evidence in the record—not even Plainfield's testimony—contradicted Gonzalez's probable cause statement and testimony that metadata (including timestamps) can be stripped from files in a cell phone, and thus that a search that did not include non-timestamped files risked missing evidence relevant to the alleged sexual assault within the timeframe listed in the warrant. The trial court determined that Acevedo, Gonzalez, and Hoskins acted in objective good faith after observing their testimony, and "[i]t is the trial court's role to evaluate witness credibility, resolve conflicts in the testimony, weigh the evidence, and draw factual inferences." (*Moore*, *supra*, 64 Cal.App.5th at p. 297.) Because the trial court's determination of historical facts was supported by substantial evidence, my " 'independent judgment' " is that the good faith exception to the exclusionary rule applies. (*Id.* at p. 296.)

The majority opinion analogizes the instant situation to that in *Nguyen*. I do not find *Nguyen* instructive in the instant case. In *Nguyen*, the warrant authorized law enforcement to search " 'a single story family residence,' " including " 'any and all yards, garages, carports, outbuildings, storage areas and sheds assigned to the above-described premises' " for evidence of computer-based child pornography. (*Nguyen*, *supra*, 12 Cal.App.5th at p. 578.) The warrant did not mention Nguyen, who lived in a separate residence behind the single family residence. (*Ibid.*) Police nonetheless searched Nguyen's residence and found a laptop containing child pornography. (*Id.* at p. 579.) The trial court granted the defendant's motion to quash the warrant and suppressed the

fruits of the search, making several findings of fact in support of its conclusion that the warrant was overbroad. (*Id.* at pp. 577, 580.) The trial court also held that police lacked a good faith basis to search Nguyen's residence because "the police knew Nguyen's residence was not a garage before they searched it, and the court found police had no basis to believe his residence had access to the suspect network." (*Id.* at p. 586.) The Court of Appeal upheld this finding, relying on the trial court's factual findings that police had no evidence prior to the search to show that Nguyen's residence shared network access with the front house that was listed in the warrant. (*Id.* at p. 587.) The Court of Appeal concluded: "Consequently, the warrant and its affidavit lacked any basis to believe the suspect network could be accessed from Nguyen's residence. Neither the warrant nor the affidavit even mentioned Nguyen or his residence. In short, nothing in the warrant or the affidavit could reasonably be interpreted as probable cause that Nguyen had actually accessed the network associated with the suspect IP address. On this record, police could not reasonably believe the warrant established probable cause to search Nguyen's residence." (*Ibid.*)

The instant case contains what the Court of Appeal found lacking in *Nguyen*: factual findings by the trial court, supported by substantial evidence, that law enforcement acted in objective good faith in exceeding the scope of the warrant, assuming the scope of the warrant was exceeded here. The trial court here found "that date and time stamps may be modified by, *inter alia*, operating system updates and that images may be scrubbed of metadata," and that Acevedo's filter to include non-timestamped files in the Cellebrite report was "arguably justified." In addition, here the trial court made factual findings concerning a factor not present in *Nguyen*—an apparent software malfunction that led to evidence allegedly outside the scope of the warrant being reviewed. The trial court in the instant case made factual findings supporting its conclusion that the good faith exception applies, and those factual findings are supported by substantial evidence. Thus, *Nguyen* does not support the conclusion that the trial court

erred in this matter in finding that the good faith exception applies on the facts of this case.

B. Law Enforcement Acted with an Objectively Reasonable Belief that the Search Was Authorized by a Valid Warrant.

Second, even assuming that law enforcement exceeded the scope of the warrant by reviewing non-timestamped images, law enforcement's actions here demonstrate that the search was " 'one directed in good faith toward the objects specified in the warrant or for other means and instrumentalities by which the crime charged had been committed' " and was not " 'a general exploratory search.' " (*Rettig*, *supra*, 589 F.2d at p. 423.) In other words, law enforcement "searched only those places and for those objects that it was reasonable to believe were covered by the warrant." (*Leon*, *supra*, 468 U.S. at p. 918, fn. 19.) In particular, Gonzalez's probable cause statement and related testimony demonstrate that law enforcement reasonably interpreted the warrant to include non-timestamped images. As the trial court noted, Gonzalez's probable cause statement specified that photographs and/or videos can be stripped of metadata, and thus Gonzalez requested permission in the probable cause statement to review all content from the device, including items with no timestamp metadata.

The majority concludes that this probable cause statement cannot be used to expand the scope of the warrant. "Generally, 'the scope of the officer's authority is determined from the face of the warrant and not from the affidavit.' [Citation.] . . . A deficient description of the place to be searched or items to be seized may be cured by reference to the affidavit where '(1) the affidavit accompanies the warrant at the time it is served, and (2) the warrant uses suitable words of reference which incorporate the affidavit by reference. [Citations.]' [Citation.]" (*People v. Ramirez* (2023) 98 Cal.App.5th 175, 193–194 (*Ramirez*).) A warrant contains a deficient description of the place to be searched or items to be seized where it is "so facially deficient that the executing officer could not reasonably presume it to be valid." (*People v. Camarella*

(1991) 54 Cal.3d 592, 596.) In the instant matter, the following language of incorporation is located at the bottom of the warrant under the magistrate's signature in a section called "Affidavit": "**Incorporation:** The facts in support of this warrant are contained in the Statement of Probable Cause and any exhibit(s), which are *attached* hereto and incorporated by reference." The majority concludes that "the search warrant is not deficient." (Maj. opn. *ante*, at p. 15.) However, the search warrant did not specify one way or the other whether non-timestamped data could be searched. The warrant authorized law enforcement to search for "[a]ll data constituting evidence and instrumentalities of sexual assaults including communications referring or relating to the above-listed criminal offenses" within the listed timeframe. This might be reasonably understood one of two ways: (1) that only files with timestamps specifically indicating the data was created or downloaded within the listed timeframe could be searched; or (2) that all data with or without timestamps could be searched, as long as it reasonably might contain evidence relevant to the alleged sexual assault during the listed timeframe. (See *Cobb*, *supra*, 970 F.3d at p. 329 [" 'a warrant may satisfy the particularity requirement *either* by identifying the items to be seized by reference to a suspected criminal offense *or* by describing them in a manner that allows an executing officer to know precisely what he [or she] has been authorized to search for and seize.' [Citation.] The warrant need not satisfy *both* criteria. [Citation.]".) As Gonzalez's probable cause statement stated, non-timestamped files may contain evidence relevant to the time period specified in the warrant, as metadata can be stripped from files. Nonetheless, regardless of whether the warrant contained a deficient description of the place to be searched or items to be seized, Acevedo testified that he was not provided the probable cause statement, and Gonzalez did not testify that he provided the probable cause statement to Acevedo. Because the prosecution did not demonstrate that the probable cause statement " 'accompanie[d] the warrant at the time it is served' " (*Ramirez*, *supra*, at p. 194), I agree with the majority's conclusion that the probable cause statement cannot expand the

scope of the warrant. In order to cure a deficient description of the place to be searched or persons or things to be seized by reference to the probable cause statement, it is important to use suitable words of incorporation in the warrant and to have the probable cause statement accompany the warrant when the warrant is served.

However, the probable cause statement is not without meaning. Gonzalez's probable cause statement evinces law enforcement's good faith effort to search for evidence responsive to the warrant and law enforcement's objectively reasonable belief that non-timestamped files were within the warrant's limits.

Gonzalez's testimony cited the probable cause statement as supporting his belief that the warrant authorized him to review files with no metadata. The majority states: "The record contains no evidence that would support a conclusion that the non-timestamped data would have fallen within the narrow date rate specified in the search warrant." (Maj. opn. *ante*, at p. 18.) However, both the probable cause statement and Gonzalez's testimony provide evidence demonstrating law enforcement's belief that non-timestamped images reasonably could contain evidence within the date and time range listed in the warrant concerning the alleged sexual assault. As the majority notes, at one point Gonzalez did testify that he realized non-timestamped files were not specifically authorized by the warrant. However, when defense counsel asked Gonzalez, "When you saw items without timestamps, did you realize that wasn't in the warrant you had obtained?" Gonzalez replied, "It was in the statement of probable cause." Gonzalez also testified that he was not aware that Acevedo selected the option to include files with no metadata in the Cellebrite report, that it is common in cases he investigated to look for images that do not contain metadata, that he assumed the images he reviewed contained some sort of timestamp, that as he reviewed the images in the Cellebrite report, he did not check to see if each image did or did not have a timestamp, and that he did not realize as he conducted the search that the raw data of the images of suspected child pornography contained dates outside the period listed in the warrant. This testimony provides

substantial evidence to support the trial court's factual finding that "it appears that [sheriff's officials] acted in objective good faith and reliance on the search warrant and affidavit, and their understanding of how Cellebrite functioned, and that exclusion of the evidence would not sufficiently deter future Fourth Amendment violations sufficiently to outweigh the costs." The "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." (*Leon*, *supra*, 468 U.S. at p. 922, fn. 23.) The warrant here did not specifically authorize law enforcement to review files with no timestamp metadata, but it also did not prohibit them from doing so. The probable cause statement and Gonzalez's testimony demonstrate that without reviewing the non-timestamped images, law enforcement could not determine whether given images contained evidence relevant to the one-month period specified in the warrant, and thus a reasonably well trained officer would believe he or she was acting within the limits of the warrant by reviewing non-timestamped files.

Law enforcement reasonably believed that the warrant permitted them to search non-timestamped images. The warrant stated that "[a]ll data constituting evidence and instrumentalities of sexual assaults including communications referring or relating to the above-listed criminal offenses" within a one-month timeframe could be searched. Law enforcement could reasonably believe that this permitted them to search non-timestamped images, because these images reasonably might contain evidence regarding the listed offense of sexual assault and evidence within the timeframe specified in the warrant, and because without reviewing such files, their investigation would be incomplete. As the cases analyzing warrants under the particularity requirement demonstrate, the reference to a specific crime makes warrants sufficiently particular. (See *Palms*, *supra*, 21 F.4th at p. 700; *Cobb*, *supra*, 970 F.3d at p. 329; *Castro*, *supra*, 881 F.3d at p. 965; *Hall*, *supra*, 142 F.3d at pp. 996–997.) Here, law enforcement reasonably could have focused on the language in the warrant authorizing them to focus on a specific allegation of sexual

assault within a listed timeframe, rather than narrowly reading the warrant to specifically authorize only the searching of files containing timestamps that fell within the listed period, leaving other evidence potentially relevant to the alleged sexual assault outside the scope of the warrant.

If the warrant had authorized law enforcement to search "all files" within a physical file cabinet relevant to a search for a crime within a specific timeframe, it would not be unreasonable to interpret the warrant to allow law enforcement to search the entire file cabinet instead of only searching file folders with dates listed on them, because other file folders beside those with dates listed on them reasonably might contain evidence relevant to the crime. (See, e.g., *United States v. Hargus* (10th Cir. 1997) 128 F.3d 1358, 1363 [government agents did not "grossly exceed the warrant" where agents were authorized by a warrant to search for "broad categories" of documentary evidence, records belonging to each category of evidence "were present in every drawer of both file cabinets," and agents effected the "wholesale seizure of file cabinets and miscellaneous papers and property not specified in the search warrant . . . ."].)

The analogy to a physical file cabinet holds true in the context of petitioner's cell phone, as numerous federal courts have recognized when rejecting challenges that warrants for computer or cell phone evidence were overbroad. (See, e.g., *United States v. Bishop* (7th Cir. 2018) 910 F.3d 335, 336–337 (*Bishop*) ["Criminals don't advertise where they keep evidence. A warrant authorizing a search of a house for drugs permits the police to search everywhere in the house, because 'everywhere' is where the contraband may be hidden. [Citations.] And a warrant authorizing a search for documents that will prove a crime may authorize a search of every document the suspect has, because any of them might supply evidence. ¶ . . . ¶ Just so with this warrant. It permits the search of every document on the cell phone, which (like a computer) serves the same function as . . . filing cabinets . . . . [Citation.]"]; *United States v. Burgess* (10th Cir. 2009) 576 F.3d 1078, 1094, fn. omitted (*Burgess*) ["[I]t is folly for a search

warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives. One would not ordinarily expect a warrant to search filing cabinets for evidence of drug activity to prospectively restrict the search to 'file cabinets in the basement' or to file folders labeled 'Meth Lab' or 'Customers.' And there is no reason to so limit computer searches. ¶ . . . ¶ . . . [I]n the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files. It is particularly true with image files."]; *United States v. Richards* (6th Cir. 2011) 659 F.3d 527, 539, fn. omitted (*Richards*) [consistent with the holding in *Burgess*, "[a]s in the case with paper documents, on occasion in the course of a reasonable search, investigating officers may examine, 'at least cursorily,' some 'innocuous documents . . . in order to determine whether they are, in fact, among those papers authorized to be seized.' [Citations.]"]; *United States v. Stabile* (3rd Cir. 2011) 633 F.3d 219, 239 (*Stabile*) [upholding a search of a hard drive folder in part "because criminals can easily alter file names and file extensions to conceal contraband"].) While these cases generally involve challenges to the scope of warrants on the grounds of lack of particularity, they nonetheless support the proposition that broad searches of computers and cell phones for relevant evidence are often necessary, and thus law enforcement in the instant case could reasonably interpret the warrant to permit them to view non-timestamped files.

The United States Supreme Court in *Riley v. California* (2014) 573 U.S. 373 (*Riley*) recognized the limits of an analogy comparing cell phones to physical files, rejecting an argument from the State that "officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart." (*Id.* at p. 400.) The Supreme Court stated: "In Riley's case, for example, it is implausible that he would have strolled around with video tapes, photo albums, and an address book all crammed into his pockets. But because each of those items has a pre-digital analogue, police under

California's proposal would be able to search a phone for all of those items—a significant diminution of privacy." (*Ibid.*) The Supreme Court also cautioned that analogizing cell phones to non-digital counterparts "would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records." (*Id.* at p. 401.) However, these statements about the concerns of comparing cell phones to analog file systems were made in the context of holding that a warrant is generally required to search digital information on a cell phone seized from an individual who has been arrested. The *Riley* court stated: "Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest." (*Ibid.*)

Here, law enforcement officials complied with *Riley* by obtaining a warrant, and later a second warrant, to search petitioner's phone. Their search of non-timestamped images falls within the good faith exception even assuming that the search exceeded the scope of the warrant. Because law enforcement would be permitted under a warrant to conduct a broad search of a physical filing cabinet for evidence of a crime during a specific timeframe, the same principle holds true for cell phones, and thus law enforcement here could reasonably interpret the warrant to permit them to search non-timestamped files. (See *United States v. Williams* (4th Cir. 2010) 592 F.3d 511, 523 (*Williams*) ["[T]he sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents"]; *Bishop*, *supra*, 910 F.3d at p. 337 ["[A]s with filing cabinets, the incriminating evidence may be in any file or folder [of a cell phone]"].) The search warrants here were obtained in the context of an evolving investigation, and law enforcement could reasonably interpret the first warrant to "authorize[] particularized but broad seizures, allowing the officers to search all areas where they might find" evidence relevant to the offense. (*People v. Helzer* (2024) 15 Cal.5th 622, 648.)

I agree with the majority that law enforcement could have included in the warrant the specific authorization to review non-timestamped files to even more particularly describe the place to be searched and the persons or things to be seized, just as the later warrant authorized law enforcement to search the "[e]ntire contents of [the] phone to include data with no date or time stamps" for evidence of sexual assault and possession of child pornography. However, the question of what law enforcement ideally could have done is separate from the question of whether the good faith exception applies on the facts of this case. Law enforcement here reasonably believed that non-timestamped files could contain evidence relevant to the alleged sexual assault within the one-month period specified in the warrant. The warrant did not prohibit law enforcement from reviewing non-timestamped files. Instead, it authorized law enforcement to obtain "[a]ll data constituting evidence and instrumentalities of sexual assaults including communications referring or relating to the above-listed criminal offenses" within a one-month timeframe. Law enforcement attempted to comply with this warrant by excluding files with timestamps outside the period listed in the warrant, while including non-timestamped files in the search because non-timestamped files reasonably might contain evidence relevant to the alleged sexual assault during the one-month timeframe listed in the warrant. "While '[o]fficers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant,' [citation], 'a computer search may be as extensive as reasonably required to locate the items described in the warrant' based on probable cause. [Citation.]" (*Burgess*, *supra*, 576 F.3d at p. 1092.)

Thus, I would hold that the People met their burden "to prove [the] officers' reliance on a warrant was objectively reasonable." (*Nguyen*, *supra*, 12 Cal.App.5th at p. 586.) Even assuming that law enforcement exceeded the scope of the warrant, the search here was not " 'a general exploratory search,' " and law enforcement did not "substantially exceed[] any reasonable interpretation of [the warrant's] provisions."

(*Rettig, supra*, 589 F.2d at p. 423.) Within the context of the historical facts determined by the trial court, my independent judgment is that law enforcement acted in objective good faith regarding the terms of the warrant in reviewing non-timestamped images. (See *Moore*, *supra*, 64 Cal.App.5th at pp. 296–297.)

C. Little to No Deterrent Effect Would be Achieved by Suppressing All Evidence Containing No Timestamp Metadata.

The majority states: "Whether the Cellebrite software malfunctioned does not ultimately affect our conclusion in this appeal." (Maj. opn. *ante*, at p. 21, fn. 18.) However, the trial court made a relevant factual finding that Cellebrite, not law enforcement, caused the creation of the non-timestamped embedded_1 files. The trial court stated: "Here, it appears that the excesses in the search were the result of, at worst, an isolated negligent failure to detect a software malfunction. Had Cellebrite not malfunctioned, the images would have had timestamps, and would have been excluded from the limited report regardless of Acevedo's use of the 'items without timestamps' filter. There was no evidence that Cellebrite routinely malfunctioned in such a manner, or had ever previously so malfunctioned."

The testimony of petitioner's own forensic investigator provided substantial evidence to support this conclusion, as he testified that: (1) Cellebrite apparently somehow created or fabricated the embedded_1 images with no metadata; (2) he had never before seen Cellebrite create a duplicate of an image and then strip it of its metadata; (3) he did not believe it is possible for someone using Cellebrite to manipulate the information being loaded into the program and thus Cellebrite, not any user of the program, "must have" created or fabricated the embedded_1 images; and (4) by analyzing the GrayKey raw data extracted from petitioner's phone, he was able to identify that the 15 images of suspected child pornography were dated before April 8, 2022, the start date of the timeframe specified in the warrant.

As the trial court concluded, but for the apparent Cellebrite malfunction creating the embedded_1 files, law enforcement would not have viewed the images of suspected child pornography, as the raw data for these files contained date stamps outside the one-month period Acevedo specified for the Cellebrite report. The record demonstrates that the issue with Cellebrite creating the embedded_1 files was an aberration not due to any misconduct on the part of law enforcement. While Acevedo testified that he specified that Cellebrite include non-timestamped files in the report in accordance with training he received from Cellebrite, Acevedo's practice of checking the box to include files with no metadata was not unreasonable, given the reality (expressed in the probable cause statement) that metadata can be stripped from files. Again, the warrant did not specifically prohibit law enforcement from reviewing non-timestamped files. As the defense expert testified and the trial court found, no evidence supported a conclusion that law enforcement did anything wrong to cause the creation of the embedded_1 files, and the defense expert testified that he had never seen Cellebrite malfunction in the way it apparently did in this matter. Substantial evidence therefore supports the trial court's factual finding that "[n]o evidence was presented to support a determination that the creation or duplication of images had previously resulted from Acevedo's extraction process."

The deterrent effect achieved by application of the exclusionary rule must be weighed against "the costs of withholding reliable information from the truth-seeking process." (*Krull*, *supra*, 480 U.S. at p. 347.) Here, where the warrant did not prohibit law enforcement from viewing non-timestamped images and where the viewing of the images of suspected child pornography resulted from a never-before-seen aberration with the Cellebrite program, any deterrent effect in applying the exclusionary rule would be minimal. Within the context of the historical facts determined by the trial court, my independent judgment is that where an isolated software malfunction resulted in the creation of the non-timestamped images law enforcement viewed, little to no deterrent

effect would be achieved by suppressing all evidence containing no timestamp metadata, when compared to the costs of suppressing evidence of a serious offense. (See *Moore*, *supra*, 64 Cal.App.5th at pp. 296–297.)

D. Law Enforcement's Actions Do Not Justify the Remedy of Suppression.

Fourth and finally, the actions of law enforcement here do not demonstrate the type of "reckless disregard of constitutional requirements" that justifies application of the exclusionary rule. (*Herring*, *supra*, 555 U.S. at p. 147.) At most, any missteps by law enforcement amounted to a misunderstanding of the limits of a vague warrant or mere negligence. The warrant did not authorize law enforcement to only view "files with metadata date stamps between" the dates listed in the warrant. Instead, it permitted law enforcement to search "[a]ll data constituting evidence and instrumentalities of sexual assaults including communications referring or relating to the above-listed criminal offenses" within a one-month timeframe. In this situation, law enforcement could reasonably interpret the warrant to encompass non-timestamped files so that they could determine if the non-timestamped files contained evidence relevant to the alleged sexual assault during the listed timeframe. (See *Williams*, *supra*, 592 F.3d at pp. 521–522 ["In this case, the warrant authorized a search of Williams' computers and digital media for evidence relating to the designated Virginia crimes of making threats and computer harassment. To conduct that search, the warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's *authorization-i.e.*, whether it related to the designated Virginia crimes of making threats or computer harassment. [Citations.] To be effective, such a search could not be limited to reviewing only the files' designation or labeling, because the designation or labeling of files on a computer can easily be manipulated to hide their substance."]; *Cobb*, *supra*, 970 F.3d at p. 329 [limiting the scope of a computer search was not "practical or prudent under the circumstances of this

investigation" where "officers had no way of knowing when they applied for the warrant exactly *what* the evidence was that Cobb sought to destroy, or *where* Cobb had placed the evidence on the computer"].) "[T]he terms of the warrant are not to be interpreted in a 'hypertechnical' manner. [Citation.] Rather, they should be read with a 'commonsense and realistic' approach, to avoid turning a search warrant into a 'constitutional straight jacket.' [Citations.]" (*Williams*, *supra*, at p. 519.)

Here, law enforcement interpreting the warrant was not required to read the warrant in a hypertechnical manner, and instead could reasonably interpret the warrant to permit it to search for non-timestamped files that reasonably could contain evidence regarding the alleged sexual assault within the listed timeframe. Gonzalez's probable cause statement and testimony demonstrate that law enforcement believed exactly this—that non-timestamped files could contain evidence relevant to the alleged sexual assault during the listed timeframe. Again, I agree with the majority that law enforcement could have included in the warrant the specific authorization to review non-timestamped files, as the later warrant to search for evidence of child pornography did. However, the failure to specify in the first warrant that law enforcement could review non-timestamped images does not demonstrate a reckless disregard for Fourth Amendment protections, particularly where the warrant did not preclude law enforcement from reviewing non-timestamped images that reasonably might contain evidence concerning the listed timeframe.

The majority focuses on Acevedo's testimony that it was his "standard protocol" to include images with no metadata when generating a Cellebrite report and on Gonzalez's testimony that he continued to review the images listed in the Cellebrite report after he realized the Cellebrite report contained items without timestamp metadata. I do not view this testimony as amounting to a reckless disregard of Fourth Amendment protections warranting the remedy of suppression. Again, as Gonzalez's probable cause statement noted, files with no timestamp metadata could contain evidence concerning the timeframe listed in the warrant. If Acevedo did not check the box to include files with no

metadata in the Cellebrite report, then the resulting report would have omitted evidence potentially relevant to the purpose of the warrant. The warrant did not specifically forbid Acevedo from including non-timestamped files in the Cellebrite report. Gonzalez's probable cause statement and testimony provide substantial evidence to support the trial court's findings "that date and time stamps may be modified by, *inter alia*, operating system updates and that images may be scrubbed of metadata," and that Acevedo's filter to include non-timestamped files in the Cellebrite report was "arguably justified." Gonzalez testified that authority to review non-timestamped images "was in the statement of probable cause," demonstrating his belief that he was authorized to review non-timestamped images. As for Gonzalez and Hoskins continuing to review images after non-timestamped images of suspected child pornography were found, while Gonzalez testified that he conducted an "extensive" search after realizing the report contained non-timestamped files, other aspects of his testimony indicated his good faith belief that he was permitted to view these images under the warrant. Gonzalez testified that as he reviewed the images in the Cellebrite report, he did not check to see if each image did or did not have a timestamp. He testified, "I'm assuming the dates were -- I mean, the images were date-stamped -- date-stamped in some sort of way." Importantly, based on the images of suspected child pornography he observed in the Cellebrite report, Gonzalez eventually sought and obtained a second search warrant for the same phone specific to items of child pornography including both timestamped and non-timestamped files, further demonstrating law enforcement's good faith efforts to comply with Fourth Amendment protections.

Law enforcement's actions do not show that they acted with the type of "reckless disregard of constitutional requirements" to justify application of the exclusionary rule. (*Herring*, *supra*, 555 U.S. at p. 147.) Rather, their actions demonstrate that they were motivated by a desire to locate evidence relevant to the sexual assault investigation that formed the basis for the warrant—evidence that could have included files both with and

without timestamp metadata. As the trial court found: "Had Cellebrite not malfunctioned, the images would have had timestamps, and would have been excluded from the limited report regardless of Acevedo's use of the 'items without timestamps' filter." If law enforcement was negligent for failing to detect the Cellebrite malfunction, mere isolated and nonrecurring negligence by law enforcement is not enough to warrant application of the exclusionary rule. (*Id.* at p. 144.) Law enforcement conducted a search of petitioner's phone to locate evidence relevant to the alleged sexual assault during the timeframe listed in the warrant, and their search did, in fact, uncover evidence relevant to the alleged sexual assault during that time. Based on the trial court's factual findings—findings supported by substantial evidence—law enforcement at worst acted negligently in failing to detect what the trial court concluded was a software malfunction resulting in the inclusion of files that law enforcement otherwise would not have viewed. Within the context of the historical facts determined by the trial court, my independent judgment is the prosecution met their burden of proving that the officers' reliance on the warrant was objectively reasonable, and that law enforcement's actions here did not rise to the level warranting the remedy of suppression. (See *Moore*, *supra*, 64 Cal.App.5th at pp. 296–297.)

IV. CONCLUSION

Given the extensive information available on modern cell phones, it is important for law enforcement to respect Fourth Amendment limitations when conducting cell phone searches. As the California Supreme Court has observed, "[w]hen it comes to electronics searches we, and the United States Supreme Court, have recognized that the degree of intrusion posed by sweeping access to such devices is great in light of their ' "immense storage capacity" ' and the highly personal nature of the information stored on them. [Citations.]" (*People v. Bryant* (2021) 11 Cal.5th 976, 990.) As the United States Supreme Court concluded in *Riley*: "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for

many Americans 'the privacies of life,' [citation]. The fact that technology now allows an individual to carry such information in his [or her] hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant." (*Riley*, *supra*, 573 U.S. at p. 403.)

Here, law enforcement attempted to respect petitioner's Fourth Amendment rights by obtaining a warrant and by excluding files with timestamps outside the listed period from the Cellebrite report, while including in their search non-timestamped files that they reasonably believed could contain evidence relevant to the scope of the warrant. This action was reasonable and both the probable cause statement and Gonzalez's testimony demonstrate that law enforcement acted in objective good faith. Nothing in the record—not even the testimony of the defense expert—rebuts the reasonableness of law enforcement's position that images without metadata might be responsive to the offense and timeframe specified in the warrant. Where law enforcement has attempted to respect the particularity requirement in the context of cell phones and then makes a reasonable interpretation of the limits spelled out in a particularized warrant, suppression is not warranted.

Suppression of evidence is "our last resort, not our first impulse." (*Hudson*, *supra*, 547 U.S. at p. 591.) The majority suppresses all evidence "that falls outside the date and time limitations listed" in the warrant. (Maj. opn. *ante*, at p. 23.) However, through no fault of law enforcement, Cellebrite created numerous duplicate images with no metadata. Had this issue with Cellebrite not occurred, law enforcement would not have viewed the images of suspected child pornography at issue here because the raw data of these images demonstrated that they contained metadata dates outside the timeframe listed in the warrant. The trial court, having heard the evidence and observed the witnesses, determined that law enforcement acted "in objective good faith and reliance on the search warrant and affidavit . . . ." The " "historical facts determined by the trial

court' " are supported under the deferential substantial evidence standard of review. (*Moore*, *supra*, 64 Cal.App.5th at p. 296.) Within the context of the historical facts determined by the trial court, my independent judgment is that the good faith exception applies. (*Ibid*.) Numerous Fourth Amendment decisions recognize that law enforcement may broadly search the files on a computer or cell phone for evidence of a specific crime pursuant to a warrant, supporting that law enforcement here acted in objective good faith in conducting their search pursuant to the warrant. (See, e.g., *Bishop*, *supra*, 910 F.3d at pp. 336–337; *Burgess*, *supra*, 576 F.3d at p. 1094; *Richards*, *supra*, 659 F.3d at p. 539; *Stabile*, *supra*, 633 F.3d at p. 239; *Williams*, *supra*, 592 F.3d at pp. 521–522.) The "last resort" remedy of suppressing all evidence containing no timestamp metadata from petitioner's phone is not warranted on the facts of this case. (*Hudson*, *supra*, at p. 591.) Therefore, I respectfully dissent.

_____

BAMATTRE-MANOUKIAN, ACTING P. J.

DiMaggio v. Superior Court (People)
H051516

Trial Court: County of Monterey

Trial Judge: Honorable Heidi K. Whilden

Counsel: Juliet Peck for Petitioner.

No appearance for Respondent.

Jeannine M. Pacioni, District Attorney, and Glenn Pesenhofer, Deputy District Attorney, for Real Party in Interest.